PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA SISTEMAS

TRABAJO DE DISERTACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERIA EN SISTEMAS

TEMA DE DISERTACIÓN:

"DISEÑO DE UNA GUÍA PRÁCTICA DE SEGURIDADES EN VoIP MEDIANTE SIP, APLICADO A LA EMPRESA CELEC EP - TRANSELECTRIC"

AUTOR:

CRISTIAN ANDRÉS FREIRE LUZURIAGA

DIRECTOR:

ING. GUSTAVO CHAFLA ALTAMIRANO

QUITO, 2014

DEDICATORIA

Dedico este proyecto primeramente a Dios por haberme dado la fuerza y la voluntad para superar momentos difíciles surgidos durante mis estudios universitarios y por haber concluido mi trabajo de fin de carrera.

También, dedico este proyecto a mis padres, hermano, abuelita y familia en general por haberme brindados su apoyo incondicional, sus valiosos y sabios consejos durante mi vida estudiantil.

AGRADECIMIENTOS

Agradezco a Dios al guiarme por el camino correcto y permitirme conseguir todas los objetivos plateados durante mi vida universitaria.

Agradezco a mis padres, hermano y abuelita los cuales significaron una parte muy importante en mi vida para seguir adelante cada día y cumplir con mis metas.

Agradezco a mis maestros por haberme brindado y compartido todos sus conocimientos durante mi carrera universitaria, a ser una persona responsable cumpliendo con todas mis tareas y principalmente haber concluido mi tesis**.**

Tabla de contenido

Índice de Figuras y Tablas

1 Capítulo I

1.1 Antecedentes

Con el transcurso del tiempo y debido al gran avance tecnológico se han ido desarrollando nuevas aplicaciones y tecnologías capaces de brindar una gran ayuda a las comunicaciones; para poder entender mejor, podemos citar a los celulares, un factor muy importante en lo que es el campo de las comunicaciones, pero lo que realmente está revolucionando es el Internet.

El Internet hoy en día, se ha convertido en un factor clave, donde cada persona se comunica por PC, celulares inteligentes (Smartphone) buscando siempre calidad del servicio en redes de datos, intercambiando correos electrónicos, mensajería instantánea, datos entre otros.

La voz sobre IP pretende mejorar los sistemas de comunicación tradicionales a mejores enfoques dentro de las telecomunicaciones, generando niveles altos de seguridad, confidencialidad, calidad y transmisión de datos de voz a través de la red, usando los mejores protocolos.

SIP está diseñado para establecer sesiones multimedia en tiempo real entre grupos de participantes tales como: voz, video llamadas, mensajería instantánea a través del protocolo IP, habilitando específicamente la integración de un completo servicio de atención de llamadas, dando mejor calidad de servicio.

La razón por la que se realiza esta investigación es para profundizar más conocimientos sobre la seguridad en VoIP, buscar posibles soluciones y mejorar las seguridades en telefonía IP.

1.2 Justificación

En la actualidad organizaciones y empresas ya optan por la seguridad en VoIP para reducir los altos costos, ampliar la cobertura manteniendo la calidad de llamada.

Para justificar el desarrollo del presente proyecto de disertación de grado, se investigará sobre las seguridades en VoIP en la empresa CELEC EP –TRANSELECTRIC, ya que no cuenta con este sistema, donde podrán beneficiarse con la investigación obtenida, ayudando a resolver problemas dentro del campo tratado, también se complementará con conocimientos nuevos y finalmente obtener un mejor servicio de calidad.

La manera de contribuir de forma metodológica es reforzar los conocimientos ya existentes con nuevos conocimientos que se obtendrán a lo largo de la investigación a realizar.

1.3 Objetivo General

Diseñar una guía práctica de seguridades en VoIP, aplicado a la empresa CELEC EP-TRANSELECTRIC

1.3.1 Objetivos específicos

1. Investigar y conocer sobre la funcionalidad de las redes VoIP
2. Investigar y conocer sobre la funcionalidad de las telefonías SIP
3. Identificar los posibles ataques que pueden suceder y las maneras de evitarlas.
4. Analizar la situación actual de la empresa CELEC EP-TRANSELECTRIC, para identificar las reales necesidades de la empresa.
5. Identificar la brecha de seguridades entre la base conceptual de VoIP y la realidad de la empresa.
6. Diseñar una guía para la seguridad de VoIP mediante SIP.
7. Describir las conclusiones y recomendaciones.

2 Capítulo II: Voz sobre IP

2.1 Introducción

En el presente capítulo hablaremos acerca de la voz sobre IP, como se lo define, sus características, sus protocolos y estándares, la arquitectura con la que funciona, la importancia de la voz sobre IP es la calidad de servicio con la que se debería trabajar, también hablaremos en qué tipo de aplicaciones funcionan y se podrá evidenciar los beneficios que otorga este tipo de tecnología.

Una segunda parte dentro de este capítulo, es la telefonía IP, su historia, sus elementos con los que trabaja y dentro de la misma sección, hablaremos sobre las centrales telefónicas con las que nos vamos a enfocar más adelante.

Un tercer punto es enfocar sobre las seguridades y vulnerabilidades que existen dentro del campo de la voz sobre IP.

Finalmente, terminaremos hablando sobre el protocolo SIP, de la misma forma que la voz sobre IP, su definición, componentes con los que está constituido.

2.2 Voz sobre Protocolo IP (VoIP)

2.2.1 Definición

VoIP, también conocido como “Voice Over Internet Protocol” es un protocolo que permite transformar las llamadas de voz “señal análogas” en señal digital para su transmisión a través de la red, digitalizando y encapsulando en paquetes IP.

La voz sobre IP es una tecnología que se ha implementado en los últimos años en las empresas y ha permitido la incorporación de nuevos servicios y un mejor rendimiento para los clientes, permitiendo ahorrar costos en llamadas fijas y brindando una comunicación más eficiente.

VoIP es capaz de transportar todo tipo de datos como: la voz y video sin disponer de una infraestructura convencional. VoIP, ofrece varios servicios ahorrando gastos en

infraestructura y manteniendo niveles altos de seguridad, fiabilidad y calidad de servicio (QoS).

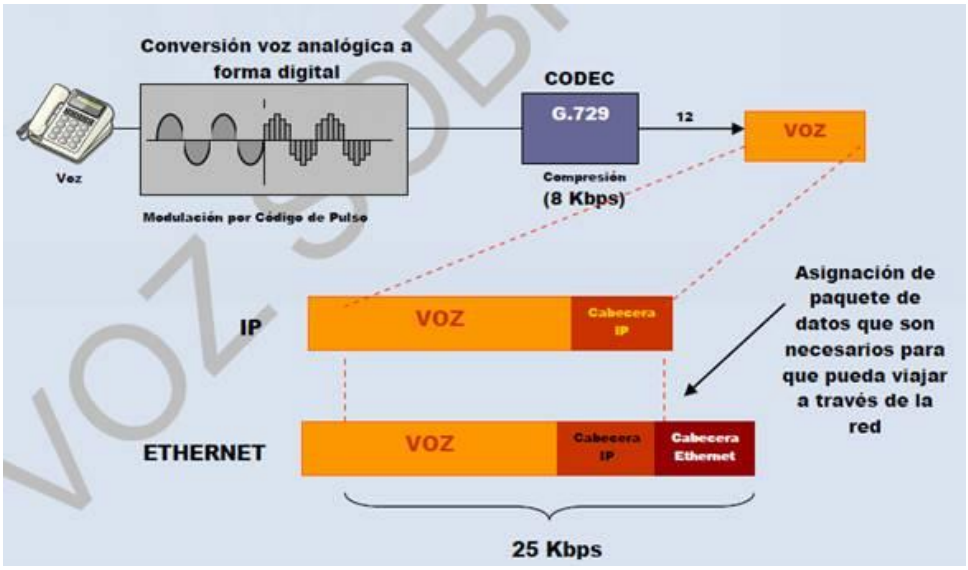


Figura 2.2.1.1 Ejemplo Voz sobre IP

(CUEVA, 2012)

2.2.2 Arquitectura de una red Voz sobre IP

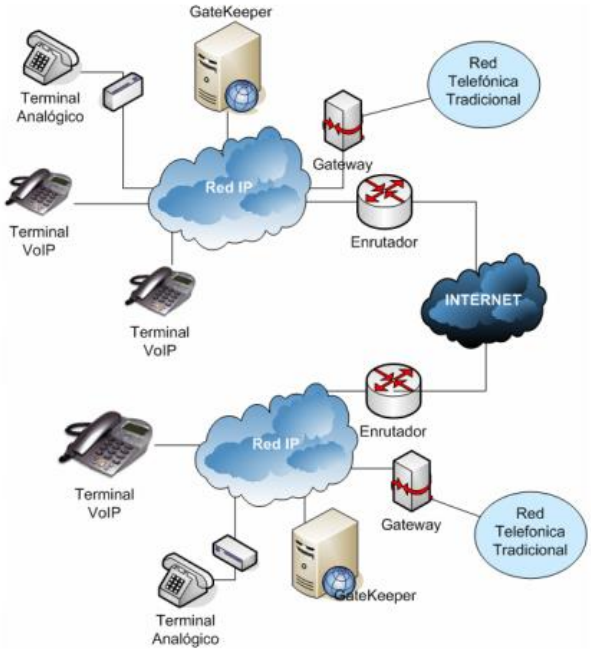


Figura 2.2.2.1 Ejemplo Arquitectura Voz sobre IP

La arquitectura de una red de Voz sobre IP se basa fundamentalmente en tres elementos muy importantes.

Terminales

Son dispositivos usados para la comunicación por los clientes conocidos normalmente como los teléfonos tradicionales.

Gateways

Son dispositivos capaces de proporcionar una conexión de comunicación entre los usuarios, estos equipos son los encargados de transformar el tráfico de datos a través de la red. Un ejemplo claro son las llamadas de voz que se las realiza en tiempo real.

Dentro de las funcionalidades de los Gateways se puede realizar controles de calidad de servicio y seguridades de acceso.

GateKeepers

Son el centro de toda la organización de Voz sobre IP y pueden ser útiles como son las centrales telefónicas, que se encargan de verificar tareas como la autenticación de usuarios, la administración de ancho de banda, entre otros.

2.2.3 Parámetros de voz sobre IP

Una de las principales razones para utilizar el servicio de Voz sobre IP es garantizar la calidad de la comunicación sobre una red IP tomando en cuenta aspectos como retardos, perdida de paquetes y anchos de banda. Para ello, la voz sobre IP se basa en algunos parámetros importantes detallados a continuación:

2.2.3.1 Códec

La función principal del códec es convertir la señal de audio/video análoga en señal digital, el códec se encarga de codificar y comprimir dicha señal para posteriormente decodificarla y descomprimirla a señal de audio. El códec es una parte esencial dentro de la VoIP y su

principal reto está en no perder la calidad de voz, evitar que ésta se entrecorte y optimizar un adecuado ancho de banda.

2.2.3.2 Tipos de códec más utilizados

- G.711

  Es un estándar de codificación de audio que no dispone de licencia y es gratuito, es uno de los códec más utilizados ya que ofrece una alta calidad de comunicación entre los dos extremos. Este códec consume demasiado ancho de banda en comparación de otros.

  Por ser gratuito, se lo pude utilizar libremente en aplicaciones VoIP. Su implementación es sencilla y no necesita de gran potencia en el CPU para ofrecer calidad de audio.

- G.729

  Es un estándar de codificación de audio de pago que también se los utiliza para la comunicación IP. Al ser un códec de pago, se necesita de una licencia que disponga ambos extremos de la comunicación.

  La ventaja que mantiene es el equilibrio en ancho de banda, calidad de audio, nivel bajo en perdida de paquetes de datos.

2.2.4 Calidad del servicio (QoS)

La calidad de servicio se considera un aspecto importante dentro de una red de voz sobre IP, ofreciendo a los usuarios la necesidad de ahorrar costos, manteniendo calidad en la conexión de llamada, calidad de la voz y tratar de brindar el mismo servicio que la telefonía tradicional.

Existen ciertos inconvenientes por lo que el servicio no es óptimo y viene a darse por lo siguiente:

- Internet: Se considera el intercambio de paquetes que viajan por un mismo camino.

- Comunicaciones VoIP que funcionan en tiempo real y provoca problemas como:
    - Eco
    - Alto porcentaje de pérdida de paquetes
    - Latencia
    - Jitter

2.2.4.1 Pérdida de paquetes

La pérdida de paquetes se llega a producir por descartes de paquetes que no llegan a tiempo al receptor. Tomando como ejemplo una conversación telefónica, la comunicación no va a ser clara. Para que la comunicación no disminuya, el porcentaje debe ser inferior al 1%, todo depende del códec que se utilice.(VoIPForo)

Una alternativa para evitar este problema es no transmitir silencios dentro de las comunicaciones.

2.2.4.2 Eco

El eco se puede dar debido a fallas técnicas o por fallas en los auriculares y micrófono, lo que produce que no se entienda tanto lo que no escucha como el habla.

Dentro de la VoIP es un factor importante, ya que no garantiza cierta calidad de voz esperada comparado con la red de telefonía tradicional. Para esto, existen dos posibles soluciones como: los supresores de eco y canceladores de eco capaces de disminuir este problema. (ElastixTech) (VoipForo, s.f.)

2.2.4.3 Jitter

Jitter se define como la variación de tiempo en el retraso de paquetes que logran llegar a su destino, puede darse debido a la congestión de la red, bajos niveles de bajo de ancho de banda o el retraso que existe entre paquetes al viajar por diferentes caminos y tarden en llegar a su destino.

Una alternativa es usar un jitter buffer[1], de tal manera que los paquetes se van almacenando, se reordenan y se da tiempo para que lleguen con más lentitud.

También puede ser controlado por medio de routers, firewalls asegurando que se mantenga uniforme el flujo de tráfico.

2.2.4.4 Latencia o Retardo

La latencia se considera aceptable con un retardo de 1,5 décimas de segundo, lo que no proporciona retardos importantes dentro de la comunicación. La pérdida de tramas[2] es el resultado de la congestión de la red. La latencia también se considera como el retraso de los paquetes del origen al destino

No existe posibles soluciones, algunas alternativas son el adecuado ancho de banda, priorización de paquetes, velocidades. (Martinez)

2.2.5 Características

- Por su estructura permite controlar el tráfico en la red disminuyendo posibles fallas y mejorando la red de datos.

- Voz sobre IP es una tecnología que se encarga de mejorar la comunicación a través de la red generando calidad de servicio

- Permite su implementación tanto para software como para hardware.

- Integración con video.

- Proporciona el enlace a la red telefónica tradicional.

- Su software es fácilmente instalable por medio de un servidor que cumpla las mismas funcionalidades de una central telefónica.

[1] Jitter buffer: Área de datos que gestiona los paquetes de voz en intervalos de tiempo.
[2] Trama: Es una unidad de envío de datos. Es una serie de bits que transportan información.

2.2.6 Protocolos y Estándares

VoIP incluye algunos protocolos que ofrecen los mismos servicios que la telefonía tradicional y son los siguientes:

- SIP

  Es un protocolo de señalización[3] que se utiliza en sesiones de usuario como la trasmisión de voz o chat. SIP se lo utiliza para establecer llamadas por Internet, se encarga de establecer llamadas desde cualquier parte.

- H.323

  Es un protocolo antiguo que facilita la convergencia de voz, video y datos, es considerado antiguo ya que no proporciona calidad de servicio y hay poca garantía en el transporte de datos, puede o no ser fiable.

- IAX

  Es un protocolo utilizado para manejar conexiones VoIP entre equipos Asterisk, entre servidores y clientes que también utilizan protocolos IAX, puede empaquetar múltiples sesiones dentro de un flujo de datos.

- RTP

  Es un protocolo en tiempo real que se define como un formato de paquetes estándar para el envío de audio y video en una video-conferencia.

2.2.7 Elementos

- El cliente

Este elemento establece y termina la llamada de voz, es decir, transmite la información generada por el micrófono, y por el contrario, la información se reproduce por medio de los

[3] Señalización: Permite el intercambio de información entre los usuarios y la red, a fin de que la llamada pueda ser establecida y terminada.

audífonos del usuario. Los clientes pueden utilizar Skype o la telefonía IP a través de teléfonos o computadoras.

- Los servidores

Son los encargados de administrar las bases de datos en tiempo real como: la contabilidad, distribución de actividades, servicios de directorios, recolección y enrutamiento, administraciones y el registro de los usuarios.

El software que requieren los servidores son de código abierto y trabaja bajo la licencia GPL[4] que proporciona funcionalidades de una central telefónica.

- Los gateways

Son dispositivos capaces de proporcionar una conexión de comunicación entre los usuarios, estos equipos son los encargados de transformar el tráfico de datos a través de la red.

2.2.8 Aplicaciones de Voz sobre IP

Algunas aplicaciones en las cuales podemos evidenciar el uso de la Voz sobre IP son las siguientes:

2.2.8.1 Asterisk

Asterisk software desarrollado por el sistema operativo GNU/Linux donde su plataforma es más eficiente y se lo puede obtener versiones para sistemas operativos como Microsoft Windows, Solaris y MacOSX. (Soluciones IT, 2015)

Las ventajas que ofrece Asterisk es su adaptación a cualquier sistema de telefonía permitiendo la compatibilidad con los equipos como gateways reduciendo costos en llamadas.

[4] GPL: Licencia orientada principalmente a proteger la libre distribución, modificación y uso de software

Algunas funcionalidades que ofrece Asterisk y que conocemos actualmente son: el correo de voz, música en espera, la transferencia y conferencia de llamadas, monitoreo de llamadas, grabación de llamadas, interfaz gráfica.

2.2.8.2 Skype

Es un software que permite realizar comunicaciones de texto, voz y video. Los usuarios de Skype pueden hablar gratis. La interfaz de Skype es amigable con el usuario y no tienen ningún tipo de problemas (NOVILLO, 2008)

2.2.8.3 Google Hangouts

Es una aplicación de Google, con la misma funcionalidad que las anteriores como la comunicación de texto, de voz y video, y se lo puede realizar a través de un ordenador o móvil.

2.2.9 Ventajas y Desventajas

Ventajas

Permite un ahorro de costos en las llamadas telefónicas, es una excelente ayuda para empresas que utilizan el servicio telefónico.

Al ser llamadas que se realizan a través del Internet, los teléfonos IP se comunican sin ningún problema y pueden ser administrados por su proveedor desde cualquier sitio donde exista conexión. (Telefonía Voz IP, s.f.)

Permite ahorrar cableado y utiliza dos tipos de conexiones como: el cableado tradicional RJ-11 y los IP usan RJ-45.

Las conexiones VoIP están orientadas a paquetes, cuando el usuario hace una llamada se establece una conexión sencilla entre el que llama y el receptor y dicha conexión abre varias rutas posibles para cada paquete, si en caso de que se dañe alguna parte entre los dos puntos de comunicación, los paquetes podrán llegar a sus destinos a través de rutas alternativas.

Desventajas

Robo de datos, un hacker puede tener acceso a la información del servidor, obtener los datos almacenados y hacer cualquier tipo de actividades ilícitas que ellos desean. (Wikipedia, 2015)

Virus dentro del sistema, los equipos pueden llegar a infectarse a tal punto que el servicio telefónico puede quedar interrumpido y las llamadas no se podrán realizar.

En ocasiones los paquetes de datos no llegan a su destino por lo que genera mala calidad en las conversaciones en tiempo real. (Wikipedia, 2015)

La telefonía IP al usar direcciones IP no sirve para ser ubicadas geográficamente y por tal razón, no pueden ser asociadas a llamadas de emergencia como el 911.

Los paquetes llegan fuera de secuencia, debido a la congestión de la red, al tráfico existente u otras razones.

Cuando nos referimos a envíos multimedia, correos electrónicos se debe especificar qué tipo de prioridades van a tener con relación a la voz y video dentro del aspecto de QoS.

2.3 Telefonía IP

2.3.1 Telefonía tradicional

Antecedentes

Se dice que el teléfono fue inventado en 1876 por Antonio Meucci, pero fue atribuido a Alexandar Graham Bell hasta el año 2002, después se confirmó que Alexander Graham Bell solo fue la persona que patento el teléfono.

La idea principal fue hacer audible la palabra a largas distancias de un punto a otro y establecer una relación de negocios, una relación de comunicación.

Originalmente la trasmisión se la realizó sobre un hilo de hierro, para la comunicación punto a punto, actualmente se la hace por alambre de cobre.

Su arquitectura inicial se definió cuando un usuario se comunicaba con otro usuario por medio de un mismo cable, éste cable no se compartía con otras personas (conexión punto a punto) y a través de una conmutación manual donde dichas personas se encargaban de realizar dicha conmutación.

2.3.2 Antecedentes telefonía IP

La telefonía IP es un sistema para realizar llamadas a través de Internet de forma económica y compatible con la telefonía tradicional que ya no depende del tiempo y la distancia, la cual no requiere de cableado telefónico pero utilizan la red de ordenadores o conexiones Wifi.

Entonces a la telefonía IP, se la puede definir como la transmisión de voz y datos entre dos puntos, es decir, trata de transportar la voz previamente convertida a datos, lo que da la posibilidad de realizar llamadas telefónicas a través de la red de datos. La telefonía IP también da la oportunidad de dar excelentes servicios a los empleados de cualquier empresa con sus diferentes sedes o con trabajadores móviles.

La telefonía IP no es un servicio, es un desarrollo tecnológico que encapsula la voz en paquetes, los transporta sobre la red sin disponer de circuitos conmutados[5] como lo hace la telefonía tradicional. Este funcionamiento ofrece la ventaja de tener un menor costo de capital, procedimientos simplificados, configuraciones y da una mayor integración entre las oficinas en una empresa dentro de una red corporativa.

La calidad de llamadas es equiparable o igual al de las llamadas de teléfonos tradicionales, siempre y cuando se disponga de un ancho de banda necesario para que no existan problemas en la conversación. Actúa igual que la telefonía tradicional, permite hacer llamadas a cualquier número de teléfono en cualquier parte del mundo y de igual manera recibir llamadas de cualquier parte ya sea fijo, móvil o internacional.

Algunas de las funcionalidades de la telefonía IP son:

- Poner en estado de ocupado la llamada.
- Mostrar mensajes que estén fuera de servicio.
- Desviación de llamadas a otro teléfono particular.

[5] Circuitos conmutados: Envían la información a través de un canal no compartido a lo largo de la llamada telefónica.

- Enviar llamadas directamente al correo de voz.

2.3.3 Elementos de la telefonia IP

ATA (Adaptador Telefónico Análogo)

Es un dispositivo electrónico que permite a los teléfonos analógicos normales transformar su señal analógica en protocolos de voz IP. Algunos de estos adaptadores ya vienen pre configurados y solo basta conectarlos para que comiencen a funcionar. Se crea una conexión física entre el teléfono analógico y un equipo de red de área local LAN, lo que hace que la señal se convierte y luego se comprima en paquetes para ser enviados en una red IP.

Figura 2.3.3.1 Ejemplo ATA

Como se muestra en la figura 2.2.3.2, una PC o un teléfono tradicional se conectan a un adaptador analógico a través de un cable RJ45, y este a su vez se conecta a un modem para así conectarse a Internet.

MCU (Unidad de Control Multipunto)

Es un tipo de hardware que gestiona la comunicación entre dos o más terminales audiovisuales juntos en una sola llamada de videoconferencia.

Los terminales envían toda la información que puede ser audio, video y datos que son encapsulados en el puerto del MCU y establece la conferencia en el mínimo común

denominador, es decir ajusta el ancho de banda y ajustar la calidad para que todos los puntos brinden un buen rendimiento.

Router

Es un dispositivo de hardware que establece la conexión de redes de computadoras donde asegura el enrutamiento de paquetes o determina la ruta por la que debe tomar el paquete de datos. Establece una conexión de una red local LAN con una red WAN y también trabaja redirigiendo los paquetes hacia los puertos de salida adecuados.

Conmutador

Es un dispositivo que permite la interconexión de redes de computadoras u otros dispositivos, su principal función es segmentar la red para mayor rendimiento. Se lo utiliza para conectar múltiples redes y transformarlos en una sola.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones MAC de los dispositivos alcanzables a través de cada uno de los puertos

Terminal

Son dispositivos que los usuarios utilizan para su comunicación, conocidos normalmente como teléfonos tradicionales que pueden ser hardware o software.

Gateway

Son dispositivos que se encargan de la comunicación entre los usuarios, proveen de interfaces con la telefonía tradicional apropiada.

Dentro de las funcionalidades de los Gateways podemos nombrar aspectos importantes como las seguridades de acceso, la contabilidad, el control de calidad del servicio (QoS) y el mejoramiento del mismo.

Gatekeeper

Son el centro de toda la organización de Voz sobre IP y son el principal sustituto para las actuales centrales, pudiendo ser implementados como software, en otras palabras son dispositivos que se encargan de realizar tareas de autenticación de usuarios, control de ancho de banda, servicios de facturación, entre otros.

2.3.4 Visión General de la Telefonía IP

La visión general de la telefonía IP funciona a través de un operador VoIP y el uso del Internet para realizar conexiones por medio de teléfonos IP o PC´s, permitiendo ejecutar llamadas ilimitadas y gratis, mientras que, si se quiere realizar llamadas a teléfonos tradicionales será a través de una red pública lo que significa que tendrá un costo bajo o mediano.

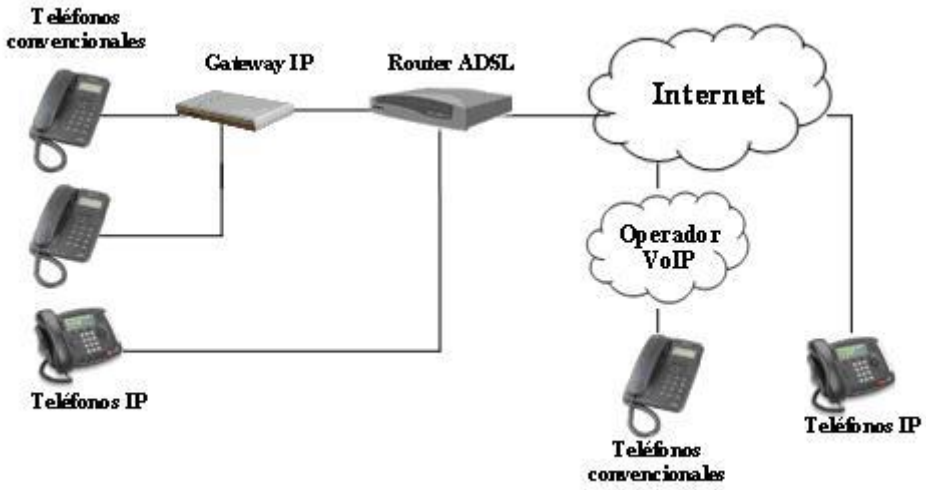


Figura 2.3.4.1 Ejemplo Visión General Telefonía IP

2.3.5 Teléfonos IP

Físicamente son dispositivos electrónicos parecidos a teléfonos normales, donde está incorporado un conector RJ45 para conectarlo directamente a una red IP en Ethernet y no pueden ser conectados a líneas telefónicas normales. Normalmente ya viene incorporado un ATA en su interior.

Para el correcto funcionamiento de este teléfono, se deberá configurar el nombre del servidor, su nombre, cuenta y correspondiente contraseña. Cada teléfono IP tiene su IP propia, y esta dirección IP puede ser asignada por el router o simplemente colocar una dirección IP estática.
Existen dos tipos te teléfonos IP:

- Basados en hardware: Similar a los teléfonos tradicionales pero ya está instalado un hardware que permite realizar y recibir llamadas a través de Internet.

- Basados en software: Hace que cualquier computador sirva como teléfono solo con usar un auricular con micrófono y/o una tarjeta de sonido y conexión a banda ancha de un proveedor VoIP o servidor SIP.

Figura 2.3.5.1 Ejemplo Teléfono IP

2.3.6 Centrales Telefónicas

Son equipos que permiten gestionar llamadas telefónicas internas dentro de una empresa y compartir líneas de acceso a la red pública entre varios puntos. La central telefónica también es conocida como Sistema Telefónico VoIP, PBX IP o servidor IP. Funciona como una ramificación de lo que es la red pública tradicional. La central telefónica es la que gestiona el ingreso y salida de llamadas. Si se requiere realizar llamadas al exterior se realizar por medio de troncales y anexos. Las llamadas son enviadas como paquetes de datos a la red en vez de la red telefónica tradicional. Los teléfonos comparten la red con las computadoras, por lo que el cableado telefónico puede ser eliminado.

Las centrales telefónicas pueden operar con teléfonos IP, proveen transferencia interna de llamadas, así como llamadas entrantes o salientes a través de la red telefónica estándar o a través de un servicio VoIP

2.3.6.1 Proveedor VoIP o Troncal SIP en una Central Telefónica

Los proveedores VoIP son aquellos que alojan líneas telefónicas y son los que están reemplazando a las líneas telefónicas tradicionales. Estos proveedores pueden asignar números locales y enrutarlos a la central telefónica. Una de sus ventajas es la reducción de costos en sus llamadas pero requiere de un ancho de banda. Como se dijo anteriormente, la VoIP se envía en tiempo real, es decir, cada llamada consume en un promedio entre 30kbps y 120kbps y dependiendo del códec.

Dentro de las centrales telefónicas existen dos tipos de proveedores como:

- Basados en registración: Se debe registrar un ID y contraseña de autentificación, por lo general ya vienen predefinidos ya que son basados en registración.

- Basados en IP o troncales SIP: La dirección IP del PBX necesita ser configurada en el proveedor, de modo que se debe enrutar las llamadas a sus números

2.3.6.2 Funcionamiento de una Central Telefónica

La central IP consiste de uno o más teléfonos basados en SIP enlazados por medio de un proveedor de servicio VoIP. Los direcciones de los teléfonos IP son registrados en la central telefónica y cuando se quiera hacer una llamada, se realiza una solicitud a la central IP para que establezca la conexión.

La central telefónica consta de un directorio de todos los teléfonos (usuarios) con sus respectivas direcciones SIP. De tal forma de conectar una llamada interna o enrutar una llamada externa a través de un proveedor VoIP.

Las centrales telefónicas incluyen una herramienta capaz de realizar un respaldo y restauración de la misma, permite crear una copia de respaldo completa de toda la configuración realizada y de los datos, para poder guardarlos en un archivo.

Dentro de las funcionalidades de la central telefónica se puede nombrar las siguientes:

- Pop up de llamada: Rechazar la llamada, transferir a otra persona o al correo de voz

- Presencia: Muestra el estado de otras extensiones, es decir permite evitar llamadas innecesarias.
- Monitoreo de colas: Ver el estado de las llamadas que están esperando.
- Chat de texto: Enviar mensajes a otros usuarios utilizando una función del chat
- Grabación de llamadas: Permite realizar un grabación de llamada
- Directorio de teléfonos: Permite guardar un listado de teléfonos de la empresa o personales

2.3.7 Ventajas de la Telefonía IP

- Optimización de recursos a través de la misma red para la transmisión de datos y voz mejorando su productividad.

- Al utilizar una red de datos da la opción a ser pública, la telefonía IP reduce los costos de operaciones y usuarios

- El acceso al servicio telefónico junto con el internet, permite tener una propia línea de cualquier punto donde solo se requiera conexión a internet.

- La virtualidad de las líneas IP hace que el riesgo de obsolescencia que sufren las redes de telefonía tradicional de una empresa por falta de funcionalidad o necesidad de ampliación de líneas o extensiones desaparezca.

2.4 Seguridad en las comunicaciones IP

Las comunicaciones IP están implementadas dentro de las empresas ofreciendo seguridad a la voz, video y datos a través de la red IP, reduciendo costos y aumentando la productividad de la empresa.

Dentro de las comunicaciones IP podemos considerar tres elementos muy importantes, que son:

Privacidad: Se entiende como vías de comunicación segura. Usan tecnologías como IP Security (IPSec)[6] y SSL[7] que ayudan a mantener comunicaciones eficientes y fuertes tanto en LAN como WAN.

Protección: Proporciona sistema de defensas contra amenazas usando tecnologías como firewalls capaces de combatir amenazas que se originan tanto internamente como externamente.

Control: Proporcionan vías de sistemas de identidad y confiablidad, las cuales hacen posible que se pueda controlar el acceso a la información dentro de las empresas.

Una de las políticas de seguridad dentro de la compañías es la de proteger la integridad, privacidad y disponibilidad con el fin de evitar errores que puedan afectar al sistema.

Una política de seguridad no solo implica tener tecnología avanzada en la alta seguridad, sino que comprende procesos operacionales que aseguren un rápido despliegue de parches (modificaciones) para software y aplicaciones.

2.4.1 Seguridades dentro de la Voz sobre IP (VoIP)

Principalmente dentro de un sistema de Voz sobre IP cuando hablamos de seguridad se obtiene algunas limitaciones con el único de propósito de ahorrar dinero e incrementar la productividad de la empresa. Los servidores de VoIP actúan como puertas de enlace; así, routers, teléfonos, nuevos protocolos y sistemas operativos están ahora entre mezclándose con esta nueva tecnología.

Para empresas grandes se debe tener mucho cuidado con respecto a las amenazas existentes propias de la VoIP.

Actualmente se puede encontrar suficiente información sobre los ataques de VoIP dentro del Internet, la mayoría de los ataques pueden llegar a producirse a nivel de aplicaciones, que para la mayoría se basa en el protocolo SIP, el cual sirve para la señalización de telefonía, conferencia, notificar eventos, mensajería instantánea con el uso del Internet.

[6] IPSec: (IP security) Servicios de seguridad de cifrado para proteger las comunicaciones a través de redes IP

[7] SSL: (Secure Socktes Layer-Capa de conexión Segura) Protocolo de seguridad para la conexión segura entre un cliente (navegador) y un servidor (computadoras con páginas web).

Formas en las que se puede manejar una adecuada seguridad es a través del uso de cortafuegos (Firewalls) o VPN (redes privadas virtuales) las cuales son utilizadas dentro de la capa de transporte del VoIP y con la ayuda del protocolo SIP se puede controlar aplicaciones Web y correo electrónico con métodos como SMTP[8] y el HTTP[9].

Firewalls: Es un software que se encarga de abrir o cerrar los puertos que se utilizan en las aplicaciones. Su función principal es impedir que hackers obtengan acceso al otro equipo a través de la red. Un firewall no se considera un antivirus pero protege de igual manera al equipo.

VPN: También denominada Red Privada Virtual**,** permite poder conectar dos equipos o más de manera segura a través de Internet, los datos son encapsulados y encriptados cuando de envía de un punto a otro. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con las mismas funcionalidades, seguridades y políticas de una red privada.

IPSec: Es uno de los protocolos de seguridad más importantes que proporciona servicios de seguridad en la capa de red y transporte tanto en TCP[10] como UDP[11] para proteger las comunicaciones a través de la redes IP, para que la comunicación sea segura, usa servicios de confidencialidad, integridad y autenticación por lo que se garantiza las comunicaciones.

2.4.2 Amenazas dentro del VoIP

Cuando nos referimos a amenazas que conciernen con la VoIP, los dispositivos de redes, servidores, sistemas operativos, protocolos, teléfonos y software son bastante vulnerables. Dentro de una conversación lo más valioso es la voz donde pueden ser reproducidas por personas con malas intenciones o del mismo modo la voz puede ser secuestrada, lo que significa puede ser modificada dicha conversación.

A continuación se presentarán algunas amenazas que ocurren dentro de un sistema de Voz sobre IP.

[8] SMTP: (Simple Mail Transfer Protocol) Protocolo de Internet para el intercambio de correo electrónico.
[9] HTTP: (HyperText Transfer Protocol) Protocolo de transferencia de información entre los servidores y los clientes (navegadores).
[10] TCP: Protocolo orientado a una conexión que envía flujo de datos, garantiza el envió de datos
[11] UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas.

2.4.3 IP Spoofing

IP Spoofing, también conocida como “Falsificación de direcciones IP”, es una técnica muy frecuente para obtener acceso no autorizado a diferentes máquinas, en donde un atacante envía paquetes IP de una falsa dirección de origen con el fin de disfrazarse y alterar la información. Estos ataques a menudo hacen sobrecargar las redes y dispositivos que parecen provenir de direcciones IP de origen legítimo.

Existen dos maneras en las que puede existir el IP Spoofing. La primera manera es simplemente sobrecargar o inundar un destino seleccionando paquetes desde varias direcciones que lo imitan. La segunda manera es la falsificación de la dirección IP de destino y enviar paquetes desde esa dirección a varios destinatarios diferentes en la red, los paquetes falsificados parezcan ser enviados desde la dirección IP del destino.

Cuando se trabaja dentro de empresas, se debe tener mucho cuidado ya que se utilizan más las direcciones IP en lugar de inicios de sesión y la suplantación debe ser controlada, por lo que los permisos de acceso y seguridad deben estar bien administrados.

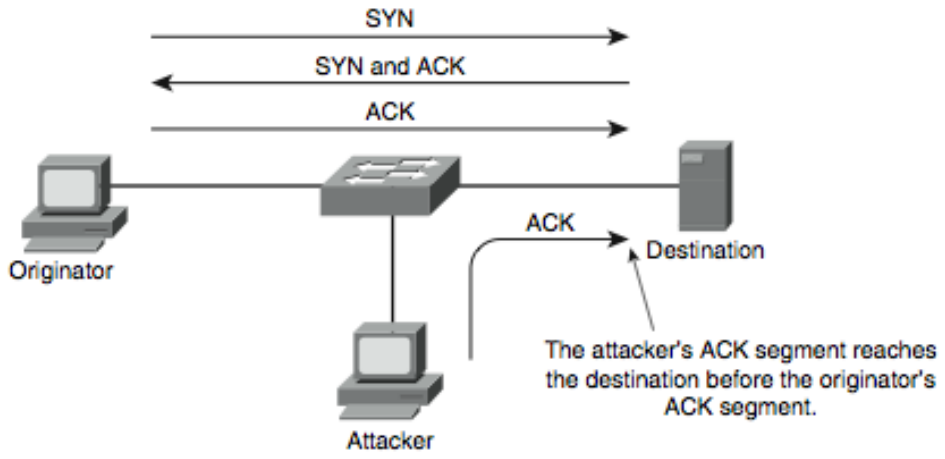


Figura 2.4.3.1 Ejemplo IP Spoofing

Es necesario recordar que el Spoofing es un ataque ciego: el atacante no ve en ningún momento las respuestas que emite su objetivo.

2.4.3.1 Defensas contra ataques de IP Spoofing

- Autentificación basada en intercambio de claves entre máquinas en nuestra red parecido a la seguridad IP (IPSec).
- Configuraciones de router y switch.
- Disponibilidad de encriptación de sesiones de router de manera que el host de confianza que esta fuera de la red se pueda comunicar de forma segura con el local host.

2.4.4 ARP Spoofing

El protocolo ARP es un protocolo de la capa de red responsable de encontrar la dirección MAC que corresponde a una determinada dirección IP.

La idea fundamental del ARP Spoofing es enviar falsos mensajes de tipo ARP a la Ethernet[12] de tal manera que una determinada máquina envíe paquetes a un host atacante en lugar de hacerlos hacia su host legítimo de destino. A este riegos también se lo puede asociar con los que es el “Hombre en la Mitad o Man in the Middle”.

El funcionamiento del ARP Spoofing es el siguiente basados en la siguiente figura:

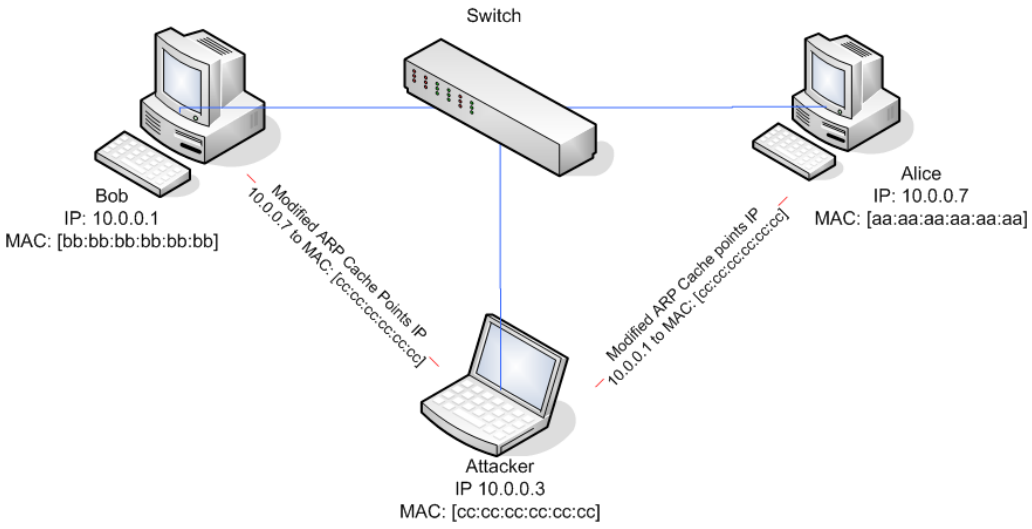


Figura 2.4.4.1 Ejemplo ARP Spoofing

[12] Ethernet: Es un estándar de conexión a la red Internet

Tenemos el host A “Bob” con una dirección IP y una dirección MAC al igual que el host B “Alice” con una dirección IP y una dirección MAC.

Cuando se hace una petición de tipo ARP REQUEST desde A hacia B se envía una respuesta indicándole la IP y MAC de A hacia B.

Después el host B responde hacia A con la misma respuesta pero con su IP y MAC propias.

EL siguiente paso es donde el host A recibe la respuesta de B, pero antes de actualizar su tabla ARP, ahí es el momento donde el atacante “Attacker” entra.

EL atacante le manda la respuesta al host A indicando que él es e host B pero con la dirección MAC del atacante.

En ese momento es donde se hizo el ARP Spoofing o se realizó un envenenamiento de la tabla ARP del host A, de tal forma que el atacante puede manejar información haciéndose pasar por otra máquina.

2.4.4.1 Defensas contra ataques de ARP Spoofing

Usar tablas estáticas, es decir, añadir entradas estáticas en lugar de dinámicas, de tal manera que cada entrada de la tabla mapea una dirección MAC con su correspondiente IP.

Otro método por el cual se puede detectar si existe un ataque es verificar que existan direcciones MAC distintas dentro de la tabla ARP.

El cambio de entradas a estáticas se las hace normalmente en los Gateway ya que por ahí se realiza el tráfico de datos pero si se conectan desde un ordenador también es recomendable.

2.4.5 SPIT o Spam VoIP

Spam de VoIP o también conocido como SPIT se lo define como el correo no deseado sobre la telefonía IP, actúa de la misma manera que un correo electrónico el cual está siendo vigilado gracias a la ayuda del filtro correo no deseado.

SPIT son mensajes no deseados o llamadas telefónicas sin importancia que se difunden a través de la VoIP a móviles conectados a Internet y suelen aparecer en las pantallas de los teléfonos IP o puede dar lugar a frecuentes timbres del teléfono.

El SPIT también puede consumir ancho de banda lo que reduce o disminuye la calidad de la llamada y la reducción de la productividad y eficiencia de los empleados.

Por el momento no es un gran problema ya que la telefonía IP no se utiliza ampliamente, pero con el tiempo el SPIT llegaría a ser un verdadero problema.

2.4.5.1 Defensas para combatir SPIT

Existen algunas maneras de evitar el problema SPIT y se nombrarán a continuación:

- Filtrado: Es el simple hecho de filtrar esta llamadas o mensajes no deseados pero se corre el riesgo de que llamadas como mensajes legítimos sean reconocidos como SPIT.

- Firewall: Es una aplicación que permite o evita ciertas llamadas aplicada más como política de seguridad dentro de las empresas. Las principales funcionalidades del firewall es evitar los ataques SIP, fraude telefónico, infecciones de virus a los teléfonos y obviamente el SPIT

- SELLO VoIP: Es una herramienta la cual detecta y bloquea el SPIT basado en patrones que se buscan dentro de la duración de la llamada, esto evitará que el teléfono suene constantemente.

- Reconocimiento de voz: Se define como una tecnología que analiza las características de la voz y las palabras de las personas con la intención de verificar si la persona es un empleado, amigo o familiar.

2.4.6 Vishing

También conocido como Phishing de VoIP, es una práctica criminal fraudulenta basada en la VoIP al igual que el SPIT trata de robar información y engañar a las personas.

Por medio de la telefonía IP, el intruso puede hacerse pasar por cualquier persona con identidad falsa para obtener información importante como los datos personales, números de cuenta, información confidencial de la víctima a través de llamadas o mensajes de texto.

2.4.6.1 Formas de evitar el Vishing

- No se debe proporcionar información si es que no se ha hecho ninguna llamada.
- No sentirse obligado a dar información sobre información confidencial.
- Pedir información sobre la persona de quien le llama, en caso de no confirmar esta persona no es legítima.
- Evitar el uso de computadoras públicas ya que existe mayor riesgo de robo de información.
- Mantener una actualización de antivirus.
- La mejor manera de evitar el vishing es por medio del sentido común y el cuidado de nuestra información personal.

2.4.7 Hacking

Por medio de personas nombradas hackers, son los encargados de tener acceso a nuestra conexión de VoIP y utilizar nuestras llamadas telefónicas con el fin de escuchar conversaciones, interrumpir las llamadas telefónica , cambiar los ID de las llamadas, capaces de insertar audio no deseado en las conversaciones y finalmente poder acceder a información confidencial o sensible del usuario.

2.4.8 Necesidad de red y Energía

No se considera una vulnerabilidad muy importante respecto a otras existentes pero cada vez que el servicio de Internet o el consumo de energía son interrumpidos también se interrumpe el servicio de VoIP, de tal manera se requiere de backup para guardar información importante.

2.4.9 Denegación de servicio (DoS)

El ataque de la denegación de servicio basado en redes VoIP se produce cuando el atacante envía múltiples paquetes a tal punto que los servicios VoIP fallan. Por lo general el DoS se centra más en el protocolo SIP el cual provoca un gran consumo de recursos en el servidor.

El robo de identidad se deriva de una denegación de servicio. Cuando se refiere al protocolo SIP, se pueden enviar mensajes de tipo CANCEL, BYE con el propósito de desconectar a los usuarios de sus propias llamadas o evitar que se produzcan nuevas llamadas impidiendo el correcto funcionamiento de dicha llamada.

Dentro de la denegación de servicio existen ataques derivados como son los siguientes:

- DoS a nivel de aplicación: La función principal de este tipo de ataque dentro de la red VoIP, es el secuestro de la sesión de cualquier teléfono IP causando la pérdida de llamadas vinculadas a otro teléfono.

- Mensajes de tipo INVITE: Es el envío de mensajes con información extraña que puede hacer que los dispositivos funciones mal o puedan dañarse por completo.

- Mensajes de tipo BYE: Cuando el identificador de llamadas funciona como un identificador único, el riesgo que puede ocurrir es cuando el atacante tiene la habilidad de cerrar la comunicación enviando mensajes tipo BYE falso al identificador de llamadas y cortar la comunicación.

- Mensajes de tipo CANCEL: La misma funcionalidad que los mensajes de tipo BYE, la comunicación llega a ser interrumpida por mensajes CANCEL que tengan el mismo valor en el campo del identificador de llamadas que tenía el mensaje INVITE de la conexión que se requiere denegar.

- DDoS: Se les denomina ataques de denegación de servicios distribuidos que son ataques simples pero con la característica que se lo realiza desde múltiples computadoras de forma coordinada.

2.4.10 Eavesdropping (Escuchas no autorizadas)

El propósito de este ataque es escuchar secretamente las conversaciones entre dos o más personas sin ser parte de dicha conversación, se debe interceptar los mensajes de señalización y el audio de la propia conversación.

Hay que tener en cuenta que los mensajes de señalización y media usan protocolos como UDP, TCP, RTP.

2.4.11 Fraude telefónico mediante VoIP

Este se considera un ataque VoIP a nivel de aplicación y consiste en tener el acceso a la red. El trabajo del atacante es suplantar el nombre de usuario y contraseñas simples e ingresando al sistema. Este tipo de fraude son los más comunes dentro del campo de la telefonía IP y son aplicadas generalmente a empresas grandes.

2.4.12 Ataques a los dispositivos

Actualmente los ataques se los realiza con el propósito principal de causar daño al hardware o software. Cuando hablamos de dispositivos centrados en las redes VoIP, podemos referirnos a los teléfonos IP, gateways que son tan vulnerables como un sistema operativo.

La mala administración y configuración de los equipos hacen que este tipo de problemas lleguen a producirse, el atacante ya tiene oportunidad de realizar cualquier daño como búsqueda de usuarios, de contraseñas, información confidencial.

2.4.13 Vulnerabilidades de la Voz sobre IP

Para poder evitar que las amenazas nombradas anteriormente tengan éxito las principales razones que pueden ocasionar son los descuidos en la mala utilización de los dispositivos, las posibles vulnerabilidades del software que se está utilizando o la arquitectura de la red por la cual se trabaja. A continuación podremos estudiar la clasificación de dichas vulnerabilidades.

2.4.13.1 Clasificación de las Vulnerabilidades de la Voz sobre IP

- Falta en la verificación de datos

  Para que los mensajes puedan evidenciarse como legítimos se debe verificar cuando se procesan los mensajes y esto incluye la verificación de la consistencia de los protocolos. Uno de los riesgos que se puede nombrar aquí es el Man in the Middle donde un intruso toma el control de una sesión, para esto, todas las conexiones a la red deben ser consideradas como hostiles y deben ser validadas.

Posibles soluciones que se pueden describir es el uso de protocolos de seguridad como IPsec, protocolo SRTP[13] para la transmisión real.

- Fallas de ejecución

Debe existir un control estricto a la hora de manejar base de datos en servidores VoIP cuando se vaya a filtrar su contenido, generalmente este proceso se aplica en soluciones de middleware[14]. Por lo tanto las fallas de ejecución se producen por un mal filtrado de datos o malas prácticas de programación. Los posibles ataques que pueden ser nombrados son suplantación o la personificación.

Posibles soluciones pueden ser buenas prácticas de programación y buscar fallas en la plataforma para que no exista vulnerabilidades y también validar nuevos software.

- Fallas de manipulación

Se produce cuando existen o se crean paquetes mal formados donde se incluye SIP, H.323 o RTP. Estos mensajes mal formados pueden ocasionar ataques de **buffer – overflow,** es decir no se controla la cantidad de datos que se copian sobre un área de memoria pre asignada y la información que sobra se almacena en memoria adyacente como registros o apuntadores y ahí es donde el intruso aprovecha para obtener información.

Mantener seguro archivos confidenciales o la autenticación de sesiones es una de las posibles soluciones para evitar vulnerabilidades.

- Pocos Recursos

Los recursos que utiliza un sistema VoIP no pueden ser limitados como la memoria o capacidad de procesamientos. Un intruso puede aprovechar enviando mensajes

[13] Protocolo SRTP: Extensión del RTP, se utilizan para el cifrado y la autenticación para minimizar los riegos de la denegación de servicios
[14] Middleware: Proporciona un enlace entre aplicaciones de software independientes

de señalización capaces de abrir sesiones internas hasta que la cantidad de sockets[15] estén completos; por lo general se realiza a través de mensajes INVITE.

- Poco ancho de banda

  Es una de las principales vulnerabilidades, cuando exista pocos usuarios no habrá ningún problema, pero a la hora de que exista demasiados usuarios el ancho de banda será muy limitado o también el ancho de banda se limita al inundar la red con peticiones para bajar el servicio.

  Para evitar esto problema, se puede combatir con la eliminación de la repetición de mensajes y manteniendo disponible el ancho de banda o a través de técnicas de QoS para mantener un servicio aceptable durante un ataque.

- Fallas debido al mal uso de archivos y recursos

  Los errores que normalmente suceden son debidos a fallas de implementación, errores de programación, prácticas inseguras de desarrollo que ocasionan que archivos del sistema, base de datos o registros tengan problemas de seguridad. Cuando se maneja información importante o confidencial se debe implementar medidas de protección de cifrado y ciertos permisos para archivos confidenciales.

- Mala gestión de contraseñas

  Dentro de VoIP, la identificación se hace a través de un número telefónico o el SIP URI[16] y la respetiva contraseña que se almacena tanto en el cliente como en el servidor y así permitiendo el acceso a la información. Algunos riesgos que se pueden nombrar son la redirección de llamadas, secuestros de sesiones o spoofing.

  Conocimientos básicos pero importantes sobre la seguridad informática, campañas de seguridad para que los empleados de las organizaciones se puede nombrar como una solución.

[15] Socket: Constituyen el mecanismo para la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos o hilos apropiados.
[16] SIP URI: Es el número telefónico del teléfono SIP de un usuario, que por lo general mantiene el siguiente formato sip:x@y:Puerto Donde x=Nombre de usuario y y=equipo dominio o IP

- Mala administración de permisos y privilegios

  Todos los recursos deben ser protegidos tanto en la arquitectura de la red como la instalación del software para mantener de forma segura y confidencial toda la información. Una buena práctica es mantener una auditoria del sistema para revisar todos los accesos y del sistema.

  Por lo tanto, se necesita una correcta administración de infraestructura tecnológica por parte de los empleados encargados en esa área, mantener capacitaciones se seguridad informática y en señalización usar protocolos seguros.

- Falta de criptografía y aleatoriedad

  Cuando hablamos de señalización en VoIP, se debe tener mucho cuidado ya que estamos hablando del eavesdropping para evitar ataques de escucha. La aleatoriedad es necesaria para designar puertos y asignar contraseñas dentro de una comunicación.

  Siempre se debe usar una buena criptografía para que los mensajes sean garantizados y a la vez usar algoritmos sofisticados y robustos.

- Manejo incorrecto de errores

  Son errores muy comunes cuando se va a implementar cualquier servicio y esto puede ser una ventaja para que un atacante o intruso puede acceder al sistema. Aquí se puede evidenciar el SPIT, spoofing, secuestro de sesiones o cuando un intruso quiere obtener registros telefónicos, es decir, este intruso intenta acceder a un teléfono que no existe, el servidor devuelve un error 404[17], pero si el teléfono devuelve un error 401[18] es donde obtiene dichos registros.

  De la misma manera usar protocolos de seguridad como IPSec y el protocolo SRTP para la transmisión de datos en tiempo real.

[17] Error 404: La página Web ya no existe en el servidor o no hay lugar dónde pueda encontrarse.
[18] Error 401: No puede acceder al sitio porque no está en la lista de invitados, su contraseña es inválida o ha ingresado su contraseña incorrectamente.

- Falta de sistemas de respaldo

  Normalmente cuando el sistema se cae, debe existir un sistema de respaldo para que los usuarios puedan volver a conectarse. Cuando hablamos de telefonía la mejor opción será colocar redes robustas para mantener los sistemas de respaldo. Los problemas que se pueden nombrar son apagones, fallas en el sistema o desastres naturales.

- Calidad de las conexiones física y colisión de paquetes

  Para que no se produzcan perdida de paquetes, latencia o jitter debe existir una buena calidad de la voz ya que se maneja en tiempo real, por lo tanto debe existir un perfecto estado en el cableado físico y una buena infraestructura.

- Comportamiento Humano

  Los usuarios son capaces de guardar contraseñas o información importante que son sitios fáciles de acceder, por lo tanto un intruso adquiere fácilmente esta información.

2.4.14 Consejos de Seguridad en VoIP

Para mantener una seguridad estable dentro de la voz sobre IP se debe considerar los siguientes consejos:

- Garantizar una infraestructura de seguridad y de red, incluyendo firewall, IDS (técnicas de detección de intrusos) y VPN que estén bien configurados para mantener este tipo de tecnología.

- Mantener estable el ancho de banda, la calidad de servicio y la latencia que son aspectos indispensables para el procesamiento de voz

- Garantizar que el sistema operativo de los conmutadores IP siempre estén actualizados para evitar recientes o nuevas vulnerabilidades.

- Cambiar cada cierto tiempo nombres de usuarios y contraseñas como control de seguridad básico.

- Mantener un monitoreo y analizar detalles sobre las llamadas que se realizan para identificar si existen llamadas telefónicas sospechosas.

- VoIP incluye protocolos de seguridad para cifrado y autenticación, pero se recomienda utilizar siempre canales seguros para proteger el tráfico de VoIP como IPSec.

2.5 SIP

2.5.1 Antecedentes y Definición

EL protocolo SIP, también conocido como Session Initiation Protocol, nació conceptualmente como un conjunto de herramientas enfocado en el establecimiento, modificación y terminación de sesiones entre usuarios en aplicaciones de voz, video, mensajería instantánea (chat) y juegos.

SIP se basa en una arquitectura cliente/servidor donde el cliente al iniciar y finalizar las llamadas. SIP se caracteriza por ser un protocolo abierto por lo que permite una gran compatibilidad. (VILLAREAL, 2006)

Su principal objetivo es la comunicación entre varios dispositivos con la ayuda de protocolos como el RTP/RTCP aquel que porta el contenido de voz y video y el protocolo SDP que describe el contenido de las sesiones. Al igual que en el correo-electrónico, las direcciones lógicas de SIP tienen la forma usuario@dominio.

2.5.1.1 Protocolo SDP

El protocolo SDP se enfoca en sesiones multimedia que permiten que los puntos de conexión participen dentro de la sesión.

El protocolo SDP requiere del nombre de la sesión, la fecha y hora de la sesión en la que está programada para iniciar, el propósito, el formato de datos, el ancho de banda,

direcciones y puertos de los puntos finales; de tal manera que las sesiones funcionen correctamente.

2.5.1.2 Protocolo RTP

Este protocolo funciona en tiempo real y transportar los datos como la voz, video a través de Internet.

El protocolo RTCP se asocia al RTP para medir el desempeño uno del otro al transmitir los datos por la red. RTP requiere de un número se secuencia, un identificador y una marca de tiempo para que se logre que los paquetes que se envían y reciben vayan en un orden correcto.

2.5.2 Componentes del Protocolo SIP

2.5.2.1 Agentes de usuario (terminales)

Los agentes de usuario son los puntos extremos del protocolo SIP, son los que emiten y consumen los mensajes. Algunos de estos terminales en software son Microsoft Windows Messenger o Apple iChat. Estas terminales se dividen en:

- Agente de usuario cliente (UAC): Es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones. Originan las solicitudes SIP.

- Agente de usuario servidor (UAS): Es una entidad lógica que genera respuestas a las peticiones SIP. Responde a la solicitud de UAC

2.5.2.2 Servidor Proxy o Proxy Server

Es el encargado de recibir las solicitudes entre el usuario cliente y los agentes usuario servidor con la intención de realizar prácticamente la petición del inicio de las llamadas y el recibimiento de dichas llamadas. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios

2.5.2.3 Servidor de Registro o Register Server

Servidor que acepta y guarda peticiones de registro de usuarios para luego suministrar el servicio de localización y dirección del dominio. Es decir, cuando un usuario inicia su terminal, el agente de usuario establece una petición REGISTER aun servidor de registro informando a que dirección física debe asociarse la dirección lógica del usuario.

2.5.2.4 Servidor de Re direccionamiento o Redirect Server

Este servidor indica al UAC (agente de usuario cliente) como encaminar el mensaje, es decir, genera una respuesta que indica al remitente la dirección del destino o de otro servidor que los acerque al destino.

2.5.3 Solicitudes y Respuestas

Como se indicó anteriormente el protocolo SIP se basa en una arquitectura de petición-respuesta, dichas peticiones son generadas por un cliente y enviadas a un servidor. Por lo tanto, SIP es aquel que proporciona un conjunto de respuestas y solicitudes.
El protocolo SIP define seis tipos de solicitudes que se definen a continuación:

Tipo	Solicitud
Invite	Establecer una session
Ack	Confirmar una solicitud invite
Bye	Finalizar una sesión
Cancel	Cancela el establecimiento de una sesión
Register	Comunica la localización de usuario como son el nombre del equipo o la IP
Options	Comunica la información acerca de las capacidades de envía y recepción de los teléfonos SIP
Info	Usada para señalizaciones de sesiones media
200OK	Envía confirmaciones satisfactorias de diferentes usuarios.

Tabla 2.5.3.1 Solicitudes Protocolo SIP

El protocolo SIP define seis tipos de respuestas que se definen a continuación:

Tipo	Respuesta
1xx	Respuestas informativas, como 180 que significa teléfono sonando.
2xx	Respuesta de éxito
3xx	Respuesta de redirección
4xx	Errores de solicitud
5xx	Errores de servidor
6xx	Errores globales

Tabla 2.5.3.2 Respuestas Protocolo SIP

Ejemplo de una llamada SIP entre dos teléfonos

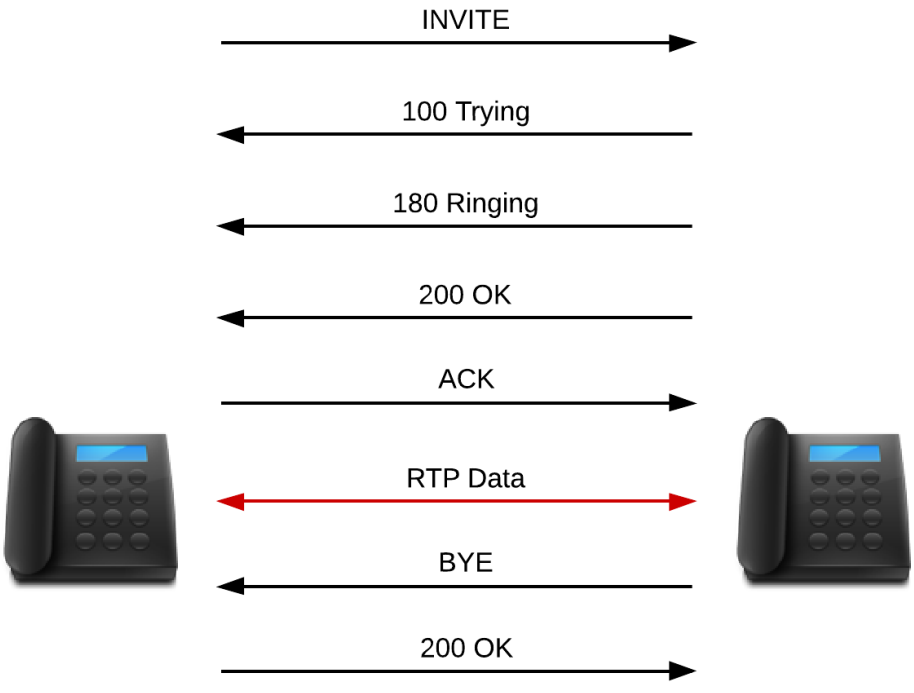


Figura 2.5.3.1 Ejemplo Llamada SIP

Pasos:

- El teléfono llamante envía un “invite”
- El teléfono al que se llama envía una respuesta informativa 100 – Tratando – retorna.
- Cuando el teléfono al que se llama empieza a sonar una respuesta 180 – sonando – es retornada.
- Cuando el receptor levanta el teléfono, el teléfono al que se llama envía una respuesta 200 – OK
- El teléfono llamante responde con un ACK – confirmado
- Ahora la conversación es transmitida como datos vía RTP
- Cuando la persona a la que se llama cuelga, una solicitud BYE es enviada al teléfono llamante
- El teléfono llamante responde con un 200 – OK.

(3CX, s.f.)

2.5.4 Beneficios del protocolo SIP

- Simplicidad: Este protocolo se caracteriza por ser muy simple ya que el desarrollo del software es corto ya que tiene similitud con HTTP y se puede reutilizar el código.

- Modularidad: Es independiente de otros protocolos, puede enviar invitaciones a las partes de la llamada, independiente de la misma sesión

- Integración: Se considera un estándar abierto, ofrece interoperabilidad entre diferentes plataformas.

- Extensibilidad: Con su similitud a HTTP y SMTP se ha construido un amplio grupo de funciones de extensibilidad y compatibilidad.

3 Capítulo III: Estudio general de la empresa CELEC EP - TRANSELECTRIC

3.1 Introducción

En el presente capítulo se realizó un estudio general sobre el sistema de comunicación con las diferentes unidades de negocio con el que trabajan actualmente, los principales protocolos con los que cuentan, el tipo de hardware que utilizan como: el tipo de central telefónica, los diferentes routers y switches que disponen y finalmente los diagramas del sistema de telefonía y de red WAN que los han implementado y trabajan actualmente.

3.2 Análisis Actual: Empresa CELEC EP - TRANSELECTRIC

Aspectos generales

La empresa CELEC EP - TRANSELECTRIC consta de tecnología de transporte donde nombraremos algunos dispositivos multiplexores como:

- SDH
    - En marcas como:
        - Siemens 7020/7030/7070
        - Huawei OSN/1500/2500/7500/3500

Estos multiplexores ocupan cables OPGW[19] que son usados en las conexiones de torre a torre. Este cable OPGW lleva por dentro un cable de fibra óptica la cual está encargada de la distribución de energía y la comunicación entre cada subestación.

También consta de un multiplexado compacto por división de longitudes de onda (DWDM) que es una técnica de transmisión de señales a través de fibra óptica y por medio de éste multiplexado se obtiene una red OTN[20].

Otro punto que podemos mencionar dentro de la empresa es la dispersión de un control de equipos que notifican de manera constante cada problema y a su vez trata de resolverlo lo más rápido posible sin ningún problema.

[19] Cable OPGW: Empleado en las líneas de transmisión y distribución de energía eléctrica, teniendo la doble función de transmisión de datos y de conexión a tierra.
[20] Red OTN: Es un conjunto de elementos de redes ópticos conectados por la misma fibra óptica

También tienen implementado un nuevo protocolo de transporte llamado MPLS encargado de transportar los diferentes tipos de tráfico incluyendo los de voz y paquetes IP. Éste protocolo les proporciona mayor fiabilidad y rendimiento, esto les permite tener una solución perfecta para las llamadas VoIP.

Consta de un servicio de internet llamado Clear Channel que permite la transmisión de datos de un sitio remoto a otra central. La empresa optó por este servicio ya que requiere de una comunicación o transmisión de datos entre sus diferentes oficinas, departamentos y que no requieran prestaciones. Realizan una comunicación vía IP a través del protocolo SIP con las diferentes centrales telefónicas existentes en el país.

Consta de un enrutamiento BGP, encargado de realizar la comunicación con el cliente y la comunicación entre las diferentes subestaciones.

Trabajan con el protocolo de mensajes VTP denominado (VLAN Trunking Protocol) encargado de la configuración y la correcta administración de la VLANs dentro de equipos dentro de la empresa, otro protocolo incorporado es el HSRP que evita que ocurra fallos en la red mediantes técnicas de redundancia y comprobación del estado de los routers. Por medio de estos protocolos, la empresa realiza sus comunicaciones entre las diferentes subestaciones en el país sin ningún problema.

3.2.1 Hardware

Además observamos que disponen con diferentes equipos como: central telefónica, switches, routers. A continuación se va a especificar de una mejor manera estos equipos.

3.2.1.1 Central Telefónica

CELEC EP – TRANSELECTRIC utiliza principalmente la central telefónica HIPATH 4000 de la marca Siemens o actualmente denominada UNIFY, con el fin de proporcionar servicios de telefonía de manera universal, de forma oportuna, confiable y eficiente tanto en el edificio principal como en las diferentes subestaciones logrando un sistema de alta disponibilidad y capacidad.

Este tipo de central telefónica fue adquirida por la empresa proveedora Hightelecom, único proveedor en proporcionar este tipo de servicios a nivel nacional. La información fue proporcionada por los mismos trabajadores.

Central telefónica Siemens HIPATH 4000 V2.0

Es una plataforma de comunicaciones capaz de mantener una alta disponibilidad, seguridad entre las comunicaciones y proporcionar la integración del flujo de trabajo, el rendimiento potente y las comunicaciones rentables.

La Siemens HiPath 4000 V2.0 ofrece un sistema de calidad de servicio en la comunicación IP. Posee la ventaja de combinar la comunicación basada en IP con los sistemas de comunicación tradicionales. Esta central telefónica está diseñada para ofrecer soluciones de comunicación en grandes empresas, ofrece diferentes opciones de disponibilidad con telefonía IP más que un sistema de telefonía tradicional.

Este centro de comunicaciones trabaja como un principio de arquitectura distribuida. Todas las aplicaciones y soluciones se las instala una solo vez y son controladas y administradas por sistema de administración central, lo cual permite un nivel alto de disponibilidad.

La plataforma está diseñada para mantener una capacidad de 300 a 12 000 líneas en un solo sistema y hasta 100 000 usuarios dentro de la red. Tiene capacidad para trabajar con gateways, terminales, aplicaciones y servicios de diferentes proveedores para proporcionar la mejor solución existente; también es fiable en cuánto a solidez y flexibilidad superior, compatible con sistemas analógicos, digitales e IP.

Características básicas

- Registro de llamadas de tráfico saliente, entrante, interna y entre redes
- Operaciones con o sin marcado interno directa
- Llamada directa
- Llamada en espera
- Timbre simultáneo
- Llamadas flexibles tales como diferentes destinos de reenvío de llamadas internas y externas
- Llamadas en grupo
- Interfaz integrada para el acceso remoto

Características de los usuarios

- Volver a marcar
- Sistema de Marcación rápida / persona
- Devolución de llamada
- Tres partidos / conferencias ocho partidos
- Conmutación
- No-molestar
- Llamada en espera y la prevención de llamada en espera
- Anulación y prevención de la anulación
- Línea Directa

Características principales

- Sistema Individual
- Sistema distribuido sobre IP
- Escalable, gran capacidad en:
    - Hasta 15 puntos de acceso conectados directamente
    - Hasta 83 puntos de acceso basados en IP adicionales
    - Hasta 12 000 usuarios digitales o IP
    - Hasta 10 000 usuarios o IP en la red

- Sistema distribuido, arquitectura escalable.
- Red IP.
- Puntos de acceso IP: basados en TDM: hasta 256 canales
- Concepto de punto de acceso de emergencia (supervivencia de los puntos de acceso IP): 40 puntos de acceso IP.
- Alta calidad de voz (por ejemplo, cancelación de eco incorporado y conmutación carga IP).
- Opción de reducción de ancho de banda
- Calidad de servicio de apoyo a través de la red IP mediante la priorización de tráfico
- DiffServ

Beneficios

- Reducción de la infraestructura de la red (Convergencia IP) para:
    - Inversiones
    - Administración
    - Administración y aplicación reduciendo costos debido a:
    - Sistema individual
    - Administración central y de aplicaciones
- Mayor alcance de funciones y aplicaciones
- Aumento de opciones debido a los puntos de acceso IP como:
    - Número
    - Escalabilidad
    - Resistencia
- Aprovechar los beneficios de una infraestructura IP sin rechazar las características riqueza, la disponibilidad y la fiabilidad.

3.2.1.2 Routers

Equipos con los que dispone la empresa dentro de sus instalaciones son los diferentes routers que tiene a su disposición y son capaces de brindar seguridad, confiabilidad, buena comunicación y acceso a Internet con suficiente ancho de banda y son los siguientes:

- Router Cisco 1800.
- Juniper SRX 220.
- Juniper MX 480.
- Juniper MX 960.

3.2.1.3 Switches

Otros equipos que están incorporados dentro de la empresa son los switches como:

- Switch Alcatel MPLS Serie 7210.
- Swicth Alcatel 7210 SAS-X.
- Swicth Alcatel 7210 SAS-M.

3.2.2 Diagrama del Sistema de telefonía CELEC EP – TRANSELECTRIC

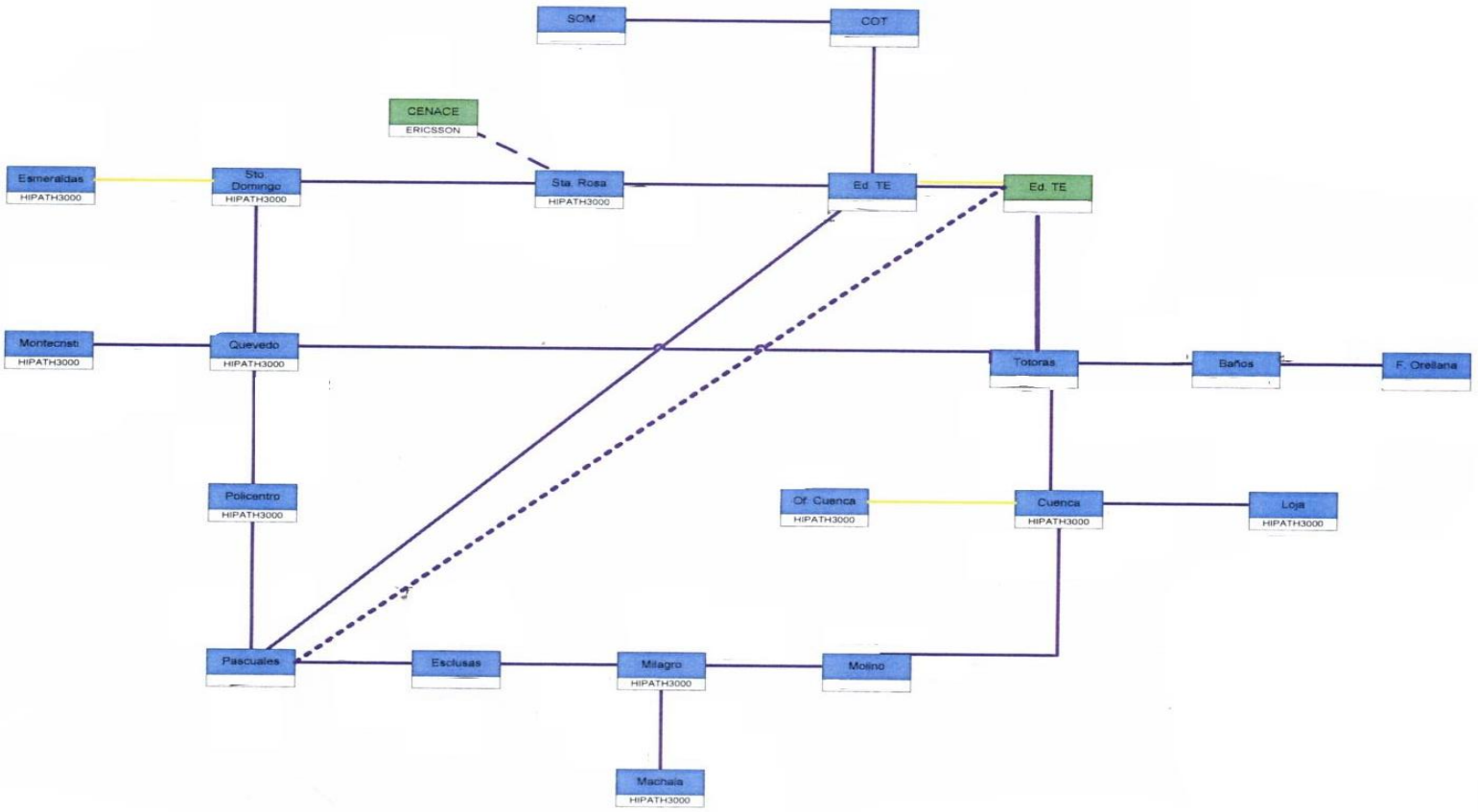
A continuación vamos a presentar un diagrama del sistema de telefonía con el que actualmente tiene la empresa CELEC EP – TRANSELECTRIC, donde observaremos cómo están conectado las diferentes centrales telefónicas ubicadas en diferentes sectores del país.

3.2.3 Diagrama de la Red WAN de CELEC EP – TRANSELECTRIC

En el siguiente diagrama se presenta el sistema de red WAN con el que actualmente tiene la empresa CELEC EP – TRANSELECTRIC, donde se observa las conexiones entre los diferentes switch y routers.

Básicamente desde los routers principales de cada subestación se establecen las conexiones a los teléfonos IP, la central telefónica correspondiente a la región, los medidores de energía, sus respectivas computadoras. Así, de igual manera, se considera la misma funcionalidad con los otros routers.

DIAGRAMA SISTEMA DE TELEFONÍA CELEC EP - TRANSELECTRIC



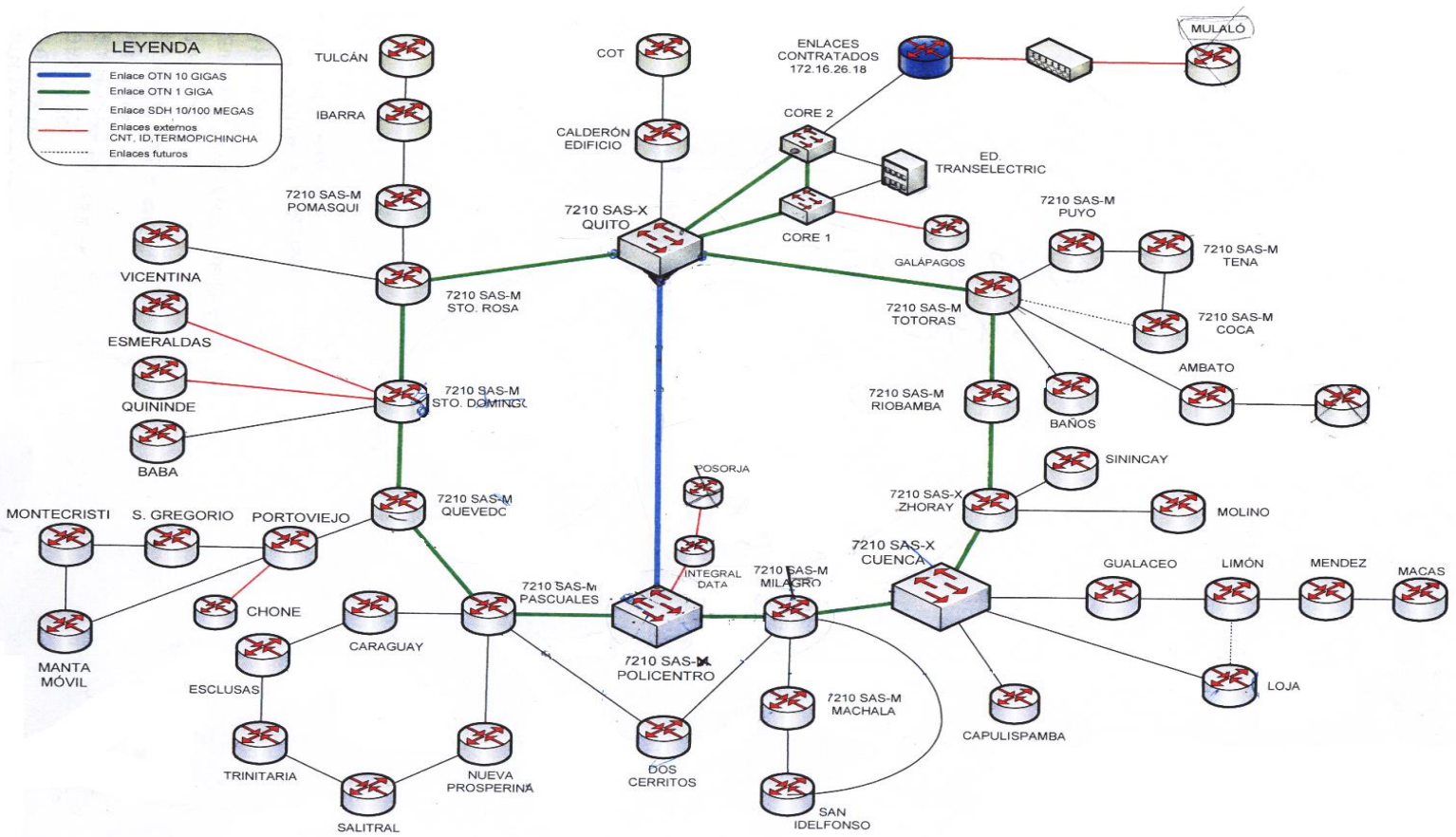
Central telefónica principal

Centrales telefónicas secundarias

Troncal E1 IP

Troncal IP

DIAGRAMA DE RED WAN CELEC EP - TRANSELECTRIC



Edificio Central

Switch Core

Router

4 Capítulo IV: Estudio de vulnerabilidades en el sistema de Telefonía IP

4.1 Introducción

En el presente capítulo se va realizar un estudio sobre el sistema de telefonía IP que dispone actualmente la empresa a través de encuestas aplicadas a los empleados y al personal técnico. Se pretende identificar problemas en la comunicación de las llamadas como: el ruido, el eco, cortes en las llamadas y en la parte técnica, identificar problemas en equipos como la central telefónica, su rendimiento, la administración de los sistemas de respaldo, calidad de servicio, algún tipo de ataque en el sistema y los mantenimientos respectivos. Finalmente los resultados serán analizados y estudiados.

4.2 Objetivos de la Encuesta

- Identificar las posibles vulnerabilidades existentes dentro la empresa
- Analizar los resultados obtenidos y dar algún tipo de solución.

Cálculo de la muestra

A continuación aplicaremos la siguiente fórmula para poder determinar la muestra e identificar la cantidad de personas a las que serán presentadas las encuestas.

$$n = \frac{M * z^2 * p * q}{e^2(M-1) + z^2 * p * q}$$

Variables	Significado	Valor
M	Tamaño de la población	400
n	Tamaño de la muestra	X
e	Margen de error	10%
z	Coeficiente de confianza	1.96
p	Probabilidad de a favor	0.5
q	Probabilidad en contra	0.5

Por lo tanto, resolviendo la fórmula obtenemos que el valor de la muestra es de **78**, es decir, a 78 personas son las que deben presentarse la encuesta.

4.2.1.1 Encuestas

Encuesta Personal

Instrucciones:

- Lea atentamente cada pregunta y responda de la mejor manera.
- Señale con una X su respuesta más apropiada

1. Indique a qué área de la empresa pertenece:

   Área de la empresa: …….

2. ¿Dispone de un reporte de llamadas realizadas desde su extensión telefónica?

   SI ( ) NO ( )

3. De ser su respuesta SI ¿Cada qué tiempo se realiza dicho reporte de llamadas?
   - Semanal ( )
   - Mensual ( )
   - Trimestral ( )
   - Anual ( )

4. ¿Ha recibido llamadas dónde usted contesta el teléfono pero no recibe ninguna respuesta?

   SI ( ) NO ( )

5. ¿Durante sus llamadas telefónicas ha tenido problemas de ruido en la comunicación?

   SI ( ) NO ( )

6. ¿Durante sus llamadas telefónicas ha tenido problemas de eco?

   SI ( ) NO ( )

7. ¿Ha tenido problemas de corte de llamadas?

   SI ( ) NO ( )

8. ¿Ha experimentado problemas de falta de tono al alzar el auricular?

   SI ( ) NO ( )

9. ¿Ha tenido problemas de retardo en las llamadas, las palabras como que tardan en llegar o recibirse?

   SI ( ) NO ( )

10. ¿Se ha suspendido el servicio telefónico alguna vez?

    SI ( ) NO ( )

11. ¿En general, está satisfecho con su servicio de telefonía?

    SI ( ) NO ( )

12. ¿Existe algún comentario/recomendación adicional que pueda realizar sobre su servicio telefónico?

    Explique:

    ……

    ……

    ……

    ……

Encuesta Técnica

Instrucciones:

- Lea atentamente cada pregunta y responda de la mejor manera.
- Señale con una X su respuesta más adecuada

1. En caso que su central telefónica produzca un daño permanente, ¿Dispone de un sistema de backup?

   SI ( ) NO ( )

2. Mantiene un sistema de respaldo de datos del sistema de telefonía fuera del que mantiene la propia central, es decir, podría levantar otra central con los datos de configuración de la actual en caso de que exista una falla permanente?

SI ( ) NO ( )

3. Cuál es el número máximo de extensión que soporto su central telefónica
   Número de extensiones: …….

4. ¿Cuántos extensiones maneja actualmente su central telefónica?
   Número de extensiones: …….

5. ¿Conoce el porcentaje de utilización de la central telefónica, en términos de proceso, es decir, cuanto del CPU se utiliza en horas pico?

   Porcentaje de utilización: …….. (%)

6. ¿La red donde funciona la central, cuanta con algún esquema de calidad de servicio para manejar los paquetes de voz y datos? Si su respuesta es afirmativa por favor explique a breves rasgos

   SI ( ) NO ( )

   ……..
   …….

7. ¿Realiza control sobre las llamadas a celulares y larga distancia desde las extensiones de los usuarios?

   SI ( ) NO ( )

8. ¿Mantienen un sistema de reportes y estadísticas para controlar las llamadas realizadas?

   SI ( ) NO ( )

9. ¿Cuántas personas son capaces de dar mantenimiento a la central?

   Número de personas: ……

10. ¿Conoce si su central telefónica ha sufrido algún tipo de ataque para denegación de servicio, por ejemplo, envío de solicitudes SIP ficticias para saturarla?

SI ( ) NO ( )

11. ¿Realiza un control de monitoreo de los protocolos de red para verificar que no se produzca algún tipo de ataque a la central telefónica? Si su respuesta es afirmativa por favor explique a breves rasgos:

SI ( ) NO ( )

Explique: ……

12. ¿Tiene contratado un servicio de mantenimiento y soporte externo para la central telefónica? Si su respuesta es afirmativa por favor explique a breves rasgos:

SI ( ) NO ( )

Explique:
……
……
……
……

13. ¿Realiza mantenimiento preventivo a la central telefónica?

SI ( ) NO ( )

1. ¿Cada qué tiempo se realiza el mantenimiento de la central telefónica?

- Semanal ( )
- Mensual ( )
- Trimestral ( )
- Semestral ( )
- Anual ( )

15. ¿Dispone de un esquema de grabación de las llamadas telefónicas?

SI ( ) NO ( )

a. Si su respuesta es SI, ¿Dónde es almacenada esa información?

……
……
……
……

b. ¿Cuánto tiempo permanecen guardada esta información?

……
……
……
……

4.2.1.2 Resultados de la Encuesta Técnica

Realizada la encuesta a nivel técnico a la persona encargada, podemos analizar la información obtenida y realizar su respectivo análisis. Los resultados que se pudieron obtener en esta encuesta, encontramos problemas como:

- Mantenimiento y soporte.
- Monitorización.
- Rendimientos de los equipos.
- Control de llamadas.
- Personal encargado.

Conclusiones:

1. CELEC EP – TRANSELECTRIC cuenta con una central telefónica en el edificio principal y consta con sistemas de respaldo que son: de alimentación, de tarjeta configurada automáticamente para su respaldo.

   En la primera pregunta consultamos si se dispone de un sistema de respaldo en caso de que se produzca un daño grave en la central telefónica, el resultado

obtenido fue negativo, por lo tanto, la información se perdió y no podrá ser recuperada ya que la central sufrió daños graves.

2. En la segunda pregunta, consultamos sí mantienen un sistema de respaldo fuera del que dispone la propia central telefónica, se podría levantar otra central con los datos de configuración actuales en caso de pérdida total, el resultado fue afirmativo y lo realizan de forma manual, se descargarán los archivos KDS (memoria de datos del cliente) almacenados y de ser necesario cargarlos en el sistema nuevamente.

3. De acuerdo a la pregunta 3, 4 y 5 se especificó el número máximo de extensiones que maneja la central telefónica, el número de extensiones que maneja actualmente y el porcentaje de utilización (proceso del CPU), los resultados obtenidos son los siguientes:

    - Número de extensiones máximo: 12 000 extensiones
    - Número de extensiones usados actualmente: 687 extensiones usadas
    - Porcentaje de utilización: 38% de utilización.

4. La sexta pregunta, si se dispone de un esquema de calidad de servicio para manejar los paquetes de voz y datos, el resultado obtenido fue negativo, no disponen de un sistema de calidad de servicio.

5. La séptima pregunta, se realiza un control de llamadas a celulares y a largas distancia desde las extensiones de los usuarios, el resultado es afirmativo, si mantienen un control de este tipo de llamadas a cada persona desde los diferentes puestos de trabajo.

6. La octava pregunta, sí mantienen un sistema de reportes y estadísticas para controlar las llamadas que suceden dentro de la empresa, el resultado fue afirmativo, pueden identificar las llamadas contestadas, ocupadas, no contestadas, registros nuevos, entre otras.

7. La novena pregunta específica cuántas personas son capaces de dar mantenimiento a la central telefónica, se dispone de 7 personas encargadas de controlar cualquier problema, en caso de que una persona no esté disponible

para reparar algún daño, existen otras personas capaces de solucionar el/los problemas.

8. La décima pregunta explica si ha tenido algún ataque a la central telefónica como por ejemplo la denegación de servicio, el resultado fue negativo, no han sufrido ningún tipo de ataque desde que se ha implementado la central telefónica.

9. La décimo primera pregunta dice si se realizaba un control de monitoreo de los protocolos de red para verificar que no se produzca algún tipo de ataque, la respuesta fue afirmativa.

    - De acuerdo a la explicación que puso el técnico fue el siguiente:
      "Existe un firewall intermedio entre comunicaciones SIP con otras centrales telefónicas de otras instituciones o unidades de negocio. En la red interna se dispone de una comunicación vía TDM (E1) con otras centrales de nuestra misma Unidad de Negocio, pero al ser una red interna controlada, sí se la monitorea con la aplicación "The Dude".

10. La décimo segunda pregunta dice si se mantiene un servicio de mantenimiento y soporte externo para la central telefónica, el resultado fue afirmativo, mantienen un servicio externo con la empresa proveedora los 5 días de la semana, 8 horas al día.

11. La décimo tercera y décimo cuarta pregunta dice si realizan un mantenimiento a la central telefónica y cada qué tiempo se le da, el resultado fue afirmativo y lo hacen anualmente.

12. La décimo quinta pregunta consulta sí la empresa dispone de un sistema de grabación de llamadas telefónicas, el resultado fue positivo. No se realiza grabaciones del resto del personal por restricciones de la normativa vigente, las grabaciones se las realiza para el COT (Centro de Operaciones de Transmisión) y próximamente para el CGTT (Dentro de Gestión de Telecomunicaciones). La información se la almacena en un tiempo de 600 horas de grabación.

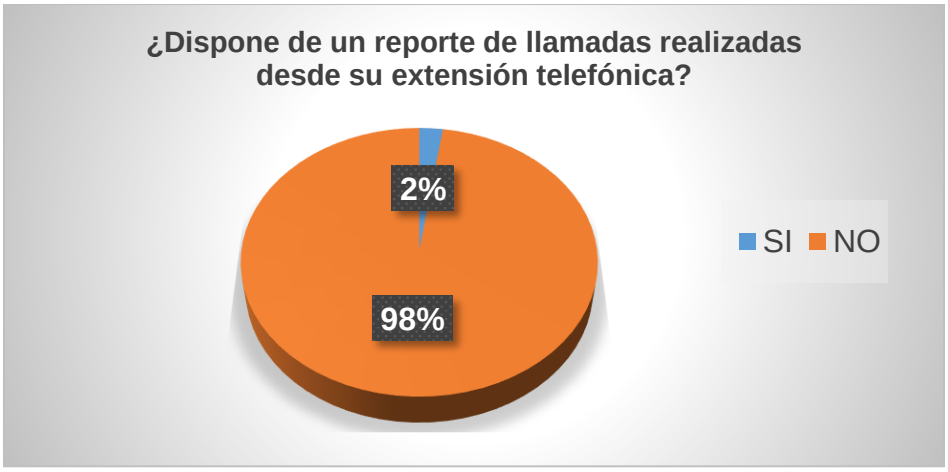
4.2.1.3 Resultados de la encuesta a usuarios.

Realizado la encuesta a usuarios podemos analizar la información obtenida y poder realizar su respectivo análisis. Las áreas de las empresas que fueron encuestadas son las siguientes:

- Subgerencia de servicios S.N.I
- Gestión social y ambiental.
- Subgerencia Jurídica
- Subgerencia de Proyectos de Expansión
- Sistema integrado de la Información

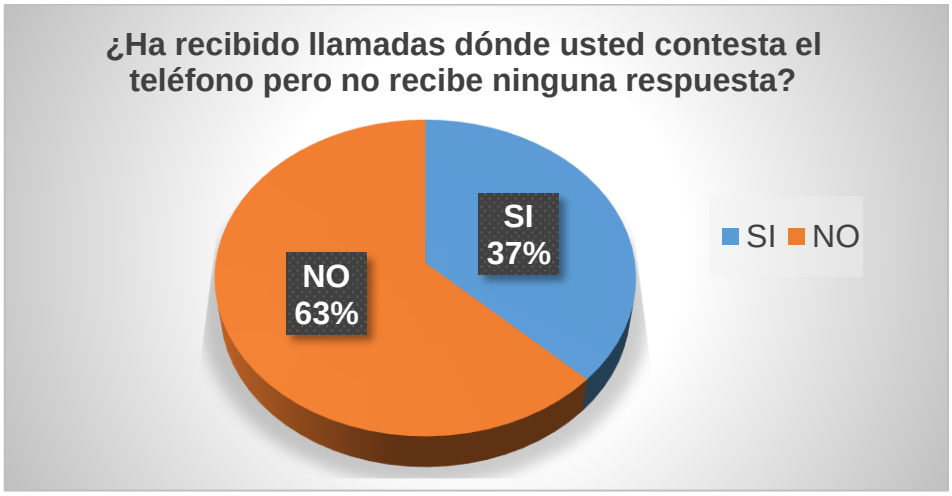
Resultados

Pregunta 1:



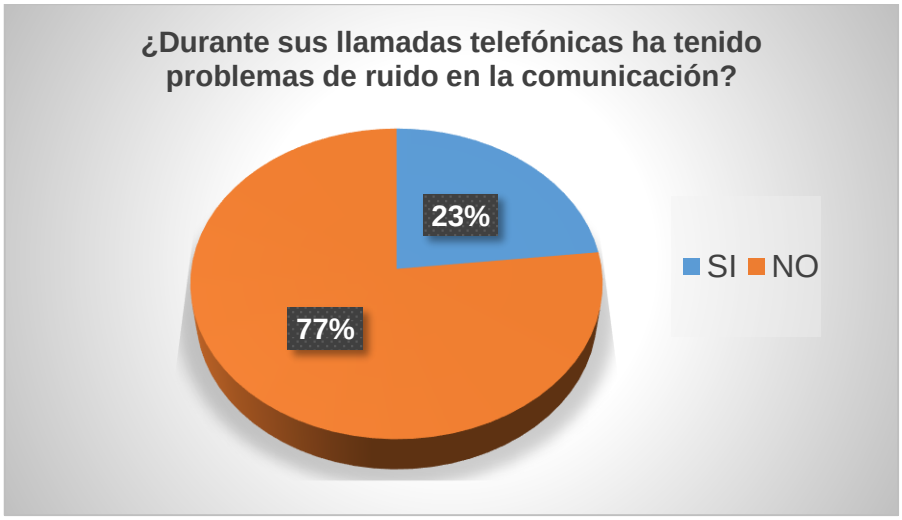
Por medio de esta pregunta podremos conocer o identificar todas las llamadas que se hacen por parte de cada persona dentro de la empresa y comprobar si realmente se hicieron dichas llamadas, caso contrario algún problema estará pasando y afectará a su vez en la parte presupuestaria.

Pregunta 2:



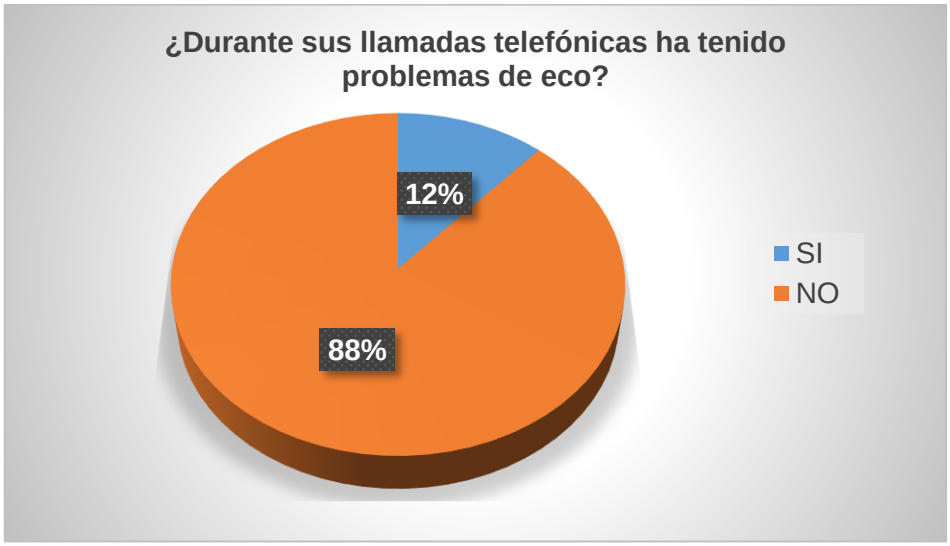
De acuerdo a los resultados de esta pregunta, podremos decir que existe un cierto porcentaje donde se contesta el teléfono pero no se recibe ninguna respuesta, esto se puede deber a que accidentalmente marcaron sin ningún propósito, fallos en la línea telefónica lo que vendría a ser un problema de seguridad.

Pregunta 3:



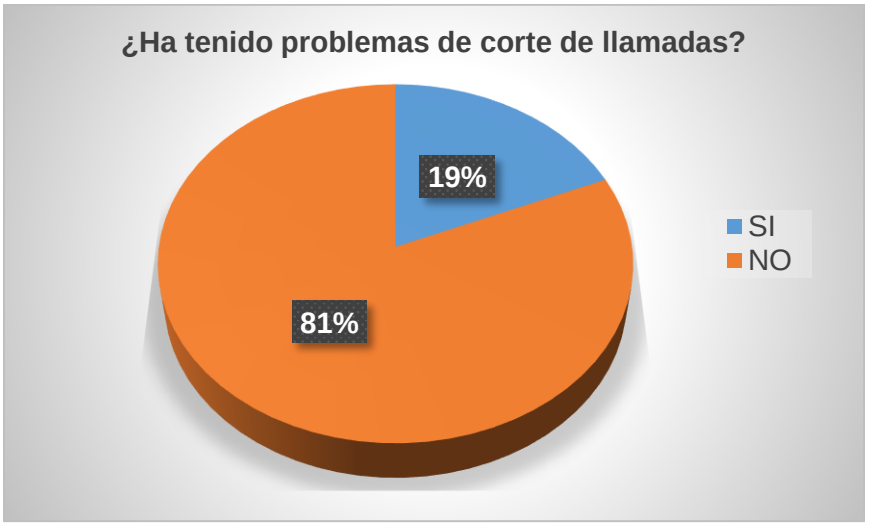
Existe un cierto porcentaje indicando que las llamadas telefónicas tienen problemas de ruido, esto puede ser que no existe calidad de transmisión en las llamadas, no existe un ancho de banda apropiado o algún problema en las configuraciones de los equipos.

Pregunta 4:



Los problemas de eco pueden llegar a darse por la falla de equipos analógicos, en este caso auriculares o micrófonos dentro de la VoIP o por la mala configuración de los gateways que son los encargados de eliminar el eco.

Pregunta 5:

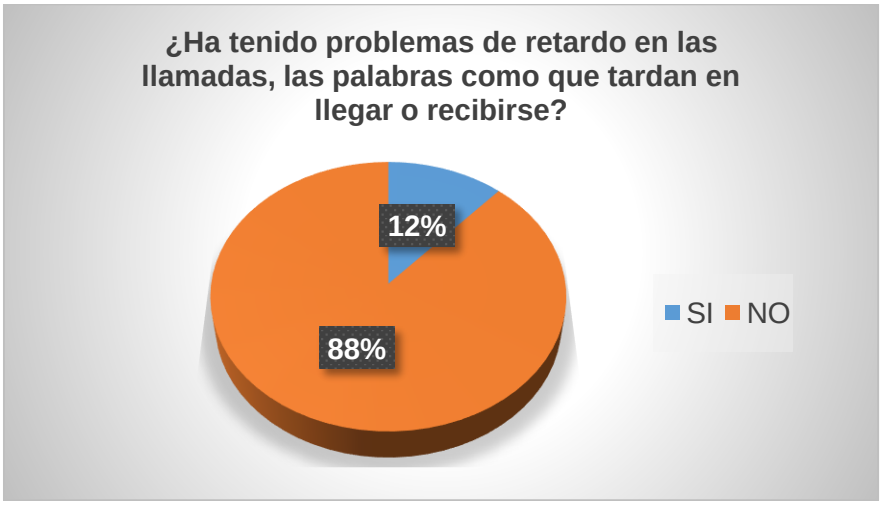


De acuerdo al porcentaje obtenido, es mínimo pero se debe llegar a solucionar. Por lo general, en su mayoría, este tipo de problemas pueden llegar a producirse debido a fallas en las líneas telefónicas, lo cual se podría solucionar rápidamente.

Pregunta 6:

Debido a un alto porcentaje por falta de tono en el auricular, por lo general este tipo de problemas se debe a su mayoría en fallas de los equipos telefónicos que vienen con defectos, para esto, se puede llamar al equipo de soporte técnico o al proveedor del servicio telefónico, también se puede comprobar que este correctamente conectado el cable telefónico de los dos extremos y finalmente comprobar que el modem funciones correctamente.

Pregunta 7:



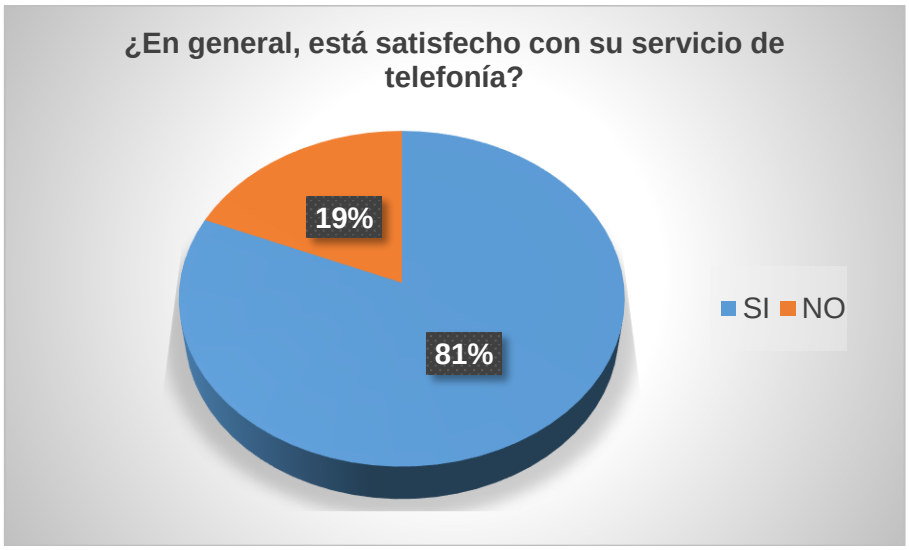
Con un mínimo porcentaje obtenido, este problema debe llegar a solucionarse, puede suceder debido baja velocidad (no existe suficiente ancho de banda) o por fallas en los router, modem o firewall que interfiere con el flujo de datos de la voz. Para poder

solucionar se requiere monitorear la red y administrar el ancho de banda para la voz sobre IP.

Pregunta 8:

Existe un porcentaje alto en cuanto se ha suspendido el servicio telefónico y puede darse por causas como la falla de conexiones entre los equipos, para esto se debe verificar que estén bien realizadas las conexiones, otros problemas puede darse a la mala configuración de los equipos.

Pregunta 9:



Al parecer en su mayoría los empleados se encuentran satisfechos con el servicio de telefonía con el que cuentan actualmente, pero con un porcentaje mínimo no están satisfechos, esto puede darse a los problemas mencionados en preguntan anteriores.

4.2.1.4 Sugerencias más importantes por parte de los empleados.

- No existe acceso a la telefonía móvil.
- No tenemos salida a celular y es muy necesario.
- Cambiar equipos telefónicos para tener un mejor funcionamiento.
- Renovación de equipos.
- Actualizar base de datos y tener un máximo de 2 personas por extensión, normalmente se utiliza hasta 6 personas por extensión.
- Entregar más extensiones y equipos.
- Deben planificar el cambio de equipos de telefonía por cuánto las teclas al presionarlas no se activan y ahí de da el caso de que por error se marca otra extensión de la que no re requiere. También por sugerencia todos los teléfonos deben brindar las extensiones de donde cubra la llamada
- Habilitar el servicio telefónico a celulares en todas las oficinas de la SPEX. La carga diaria de llamadas por y hacia celulares es alta y se lo realiza con dispositivos personales.
- Poner más extensiones al personal, son muy limitadas, deben tener uso de celulares personal es para llamadas sobre asuntos de oficina.

Una vez aplicadas las dos encuestas tanto a los empleados de la empresa como al personal técnico, se logró obtener resultados y porcentajes importantes donde se pudo evidenciar que existen problemas en el servicio de telefonía. Por lo tanto, se encontró tres vulnerabilidades muy importantes que son:

- Inhabilitación de la central telefónica al producirse algún daño grave
- Falta de calidad de servicios (QoS)
- Falta de calidad de experiencia (QoE)

La primera vulnerabilidad que obtuvimos sobre la central telefónica fue a través de la encuesta técnica, para esto debemos conocer cómo funcionan los sistemas de respaldo de esa central telefónica, se necesita tener un contrato con la empresa proveedora y si es posible tener una central espejo. Para las dos siguientes vulnerabilidades se logró

concluir a través de la otra encuesta debido a problemas con el servicio de telefonía y por consiguiente, esto se debe a que no disponen de calidad de servicios y de calidad de experiencia.

En el siguiente capítulo, vamos a tratar con más detalle estás tres vulnerabilidades.

5 Capítulo V: Análisis de resultados y sus soluciones

5.1 Introducción

E este capítulo hablaremos sobre las tres vulnerabilidades que logramos identificar en el capítulo anterior a través de las encuestas.

Para la primera vulnerabilidad identificada en cuánto a la central telefónica vamos a aportar con tres posibles alternativas para solucionar dicho problema como: la implementación de una central espejo, disponer de un contrato con la empresa proveedora (SLA) y mantener un adecuado sistema de respaldo de datos de la central telefónica.

Para la segunda vulnerabilidad identificada como la falta de disponibilidad de un sistema de calidad de servicio, se realizará un estudio sobre los actuales sistemas de calidad de servicio y que pasos se requieren para su implementación.

Finalmente, como tercera y última vulnerabilidad identificada como la falta de un sistema de calidad de experiencia, tomando en cuenta que no se dispone de pruebas de calidad de voz.

5.1.1 Vulnerabilidad 1: Inhabilitación de la central telefónica

Una de las principales vulnerabilidades que se encontró en el sistema de comunicación a través de los resultados de las encuestas, fue la falta de disponibilidad de una nueva central telefónica, en el caso de que existan daños graves en la actual central telefónica.

Para solucionar este problema, se propone adquirir, instalar y configurar una nueva central telefónica, sino también disponer de un contrato con la empresa proveedora HighTelecom con la que trabajan actualmente e indicando las necesidades que puedan cubrir este tipo de problemas y solucionarlo lo más rápido posible.

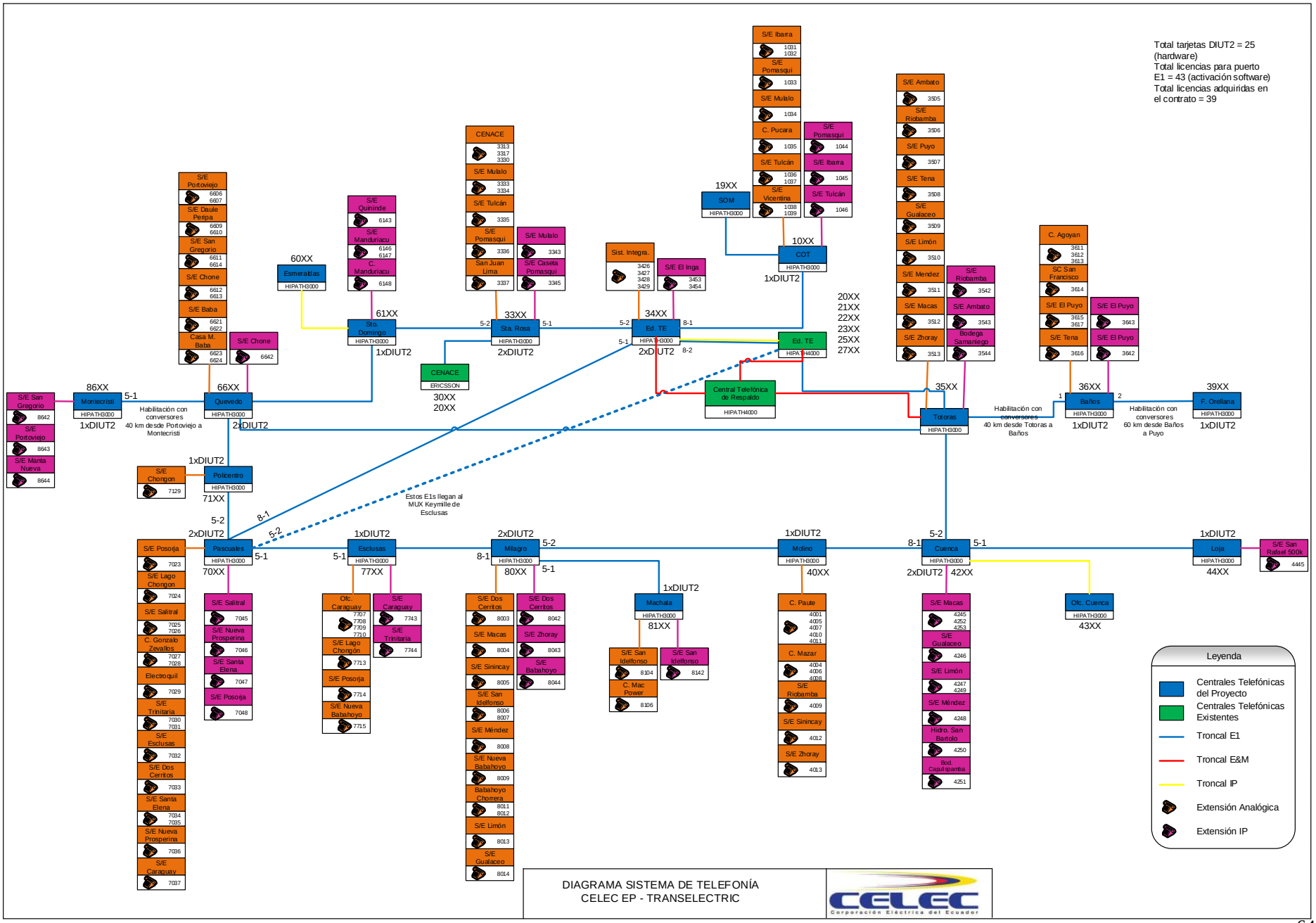
También debemos realizar una investigación y conocer cómo funcionan los sistemas de respaldo de datos de este tipo de centrales telefónicas y los gastos de las mismas. Otra opción es disponer de una central telefónica de respaldo "central espejo" que cumpla con la misma funcionalidad que la central telefónica actual con el fin de que el

sistema de telefonía no se caiga, es decir, si se llegara a dañarse la actual central telefónica automáticamente entraría a funcionar la central espejo.

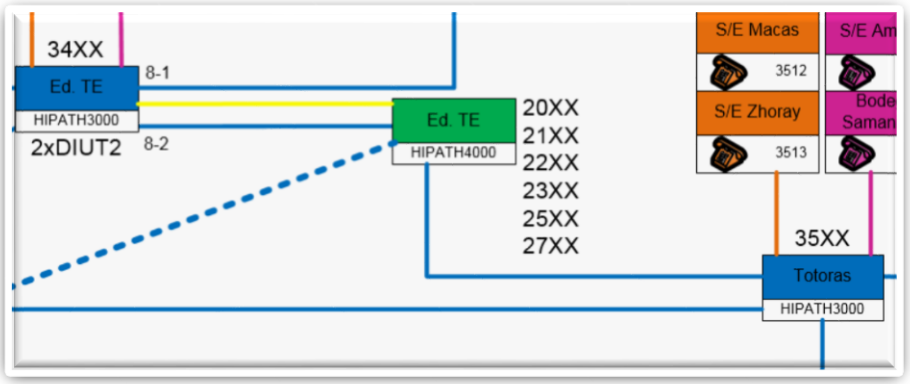
Primera Solución: Central Espejo

A continuación se presenta un diagrama del sistema de telefonía de CELEC EP TRANSELECTRIC actual donde se realizará las modificaciones correspondientes.

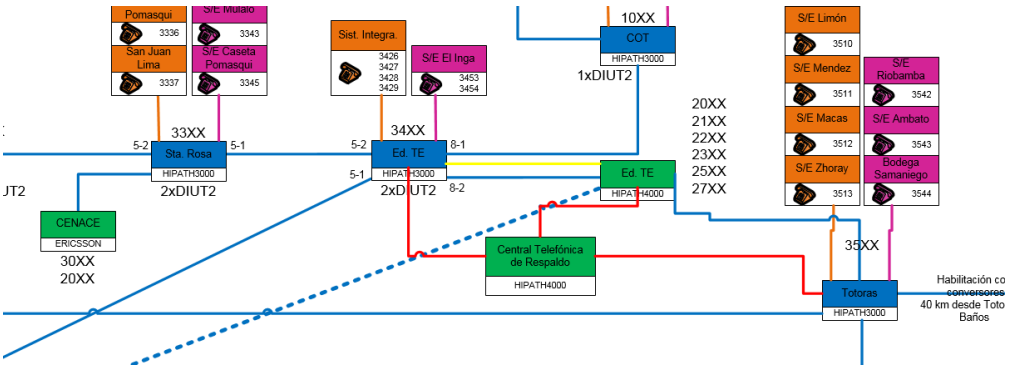
Sistema de Telefonía


Total tarjetas DIUT2 = 25 (hardware)
Total licencias para puerto E1 = 43 (activación software)
Total licencias adquiridas en el contrato = 39
S/E Portoviejo 6606 6607
S/E Daule Peripa 6609 6610
S/E San Gregorio 6611 6614
S/E Chone 6612 6613
S/E Baba 6621 6622
Casa M. Baba 6623 6624
S/E Chone 6642
S/E Quinindé 6143
S/E Manduriacu 6146 6147
C. Manduriacu 6148
Esmeraldas HIPATH3000
Sto. Domingo HIPATH3000
1xDIUT2
CENACE 3313 3317 3330
S/E Mulalo 3333 3334
S/E Tulcán 3335
S/E Pomasqui 3336
San Juan Lima 3337
S/E Mulalo 3343
S/E Caseta Pomasqui 3345
Sta. Rosa HIPATH3000
2xDIUT2
Sist. Integra. 3426 3427 3428 3429
S/E El Inga 3453 3454
Ed. TE HIPATH3000
2xDIUT2
CENACE ERICSSON
30XX 20XX
S/E Ibarra 1031 1032
S/E Pomasqui 1033
S/E Mulalo 1034
C. Pucara 1035
S/E Tulcán 1036 1037
S/E Vicentina 1038 1039
S/E Pomasqui 1044
S/E Ibarra 1045
S/E Tulcán 1046
SOM HIPATH3000
19XX
COT HIPATH3000
10XX
1xDIUT2
Ed. TE HIPATH4000
20XX 21XX 22XX 23XX 25XX 27XX
Central Telefónica de Respaldo HIPATH4000
S/E Ambato 3505
S/E Riobamba 3506
S/E Puyo 3507
S/E Tena 3508
S/E Guaiaceo 3509
S/E Limón 3510
S/E Mendez 3511
S/E Macas 3512
S/E Zhoray 3513
S/E Riobamba 3542
S/E Ambato 3543
Bodega Samanriego 3544
C. Agoyan 3611 3612 3613
SC San Francisco 3614
S/E El Puyo 3615 3617
S/E Tena 3616
S/E El Puyo 3643
S/E El Puyo 3642
Totoras HIPATH3000
35XX
Habilitación con conversores 40 km desde Totoras a Baños
Baños HIPATH3000
36XX
1xDIUT2
Habilitación con conversores 60 km desde Baños a Puyo
F. Orellana HIPATH3000
39XX
1xDIUT2
S/E San Gregorio 8642
S/E Portoviejo 8643
S/E Manta Nueva 8644
Montecristi HIPATH3000
86XX
1xDIUT2
Habilitación con conversores 40 km desde Portoviejo a Montecristi
Quevedo HIPATH3000
66XX
2xDIUT2
S/E Chongon 7129
Policentro HIPATH3000
71XX
1xDIUT2
Estos E1s llegan al MUX Keymille de Esclusas
S/E Posorja 7023
S/E Lago Chongon 7024
S/E Salitral 7025 7026
C. Gonzalo Zevallos 7027 7028
Electroquil 7029
S/E Trinitaria 7030 7031
S/E Esclusas 7032
S/E Dos Cerritos 7033
S/E Santa Elena 7034 7035
S/E Nueva Prosperina 7036
S/E Caraguay 7037
Pascuales HIPATH3000
70XX
2xDIUT2
S/E Salitral 7045
S/E Nueva Prosperina 7046
S/E Santa Elena 7047
S/E Posorja 7048
Esclusas HIPATH3000
77XX
1xDIUT2
Ofc. Caraguay 7707 7708 7709 7710
S/E Lago Chongón 7713
S/E Posorja 7714
S/E Nueva Babahoyo 7715
S/E Caraguay 7743
S/E Trinitaria 7744
Milagro HIPATH3000
80XX
2xDIUT2
S/E Dos Cerritos 8003
S/E Macas 8004
S/E Sinincay 8005
S/E San Idelfonso 8006 8007
S/E Méndez 8008
S/E Nueva Babahoyo 8009
Babahoyo Chorrera 8011 8012
S/E Limón 8013
S/E Guaiaceo 8014
S/E Dos Cerritos 8042
S/E Zhoray 8043
S/E Babahoyo 8044
Machala HIPATH3000
81XX
1xDIUT2
S/E San Idelfonso 8104
C. Mac Power 8106
S/E San Idelfonso 8142
Molino HIPATH3000
40XX
1xDIUT2
C. Paute 4001 4005 4007 4010 4011
C. Mazar 4004 4006 4008
S/E Riobamba 4009
S/E Sinincay 4012
S/E Zhoray 4013
Cuenca HIPATH3000
2xDIUT2 42XX
S/E Macas 4245 4252 4253
S/E Guaiaceo 4246
S/E Limón 4247 4249
S/E Méndez 4248
Hidro. San Bartolo 4250
Bod. Capulispamba 4251
Ofc. Cuenca HIPATH3000
43XX
Loja HIPATH3000
44XX
1xDIUT2
S/E San Rafael 500k 4445
Leyenda
Centrales Telefónicas del Proyecto
Centrales Telefónicas Existentes
Troncal E1
Troncal E&M
Troncal IP
Extensión Analógica
Extensión IP
DIAGRAMA SISTEMA DE TELEFONÍA
CELEC EP - TRANSELECTRIC
CELEC
Corporación Eléctrica del Ecuador

Como se observa en la primera imagen, se puede apreciar que están conectadas tres centrales telefónicas: la central Ed. TE, la central Ed. TE y la central Totoras por medio de troncales E1. Esta imagen es el diseño original de cómo está conectada las tres centrales telefónicas.



Para el diseño modificado es implementar una central telefónica espejo. En el caso de que la central telefónica llegase a tener un daño grave, la conexión con las otras centrales se perderá y se caerá el sistema de telefonía general, para esto la implementación de la central telefónica espejo permitirá reemplazar automáticamente a la central original y mantener funcionando la conexión con las otras dos centrales adyacentes. Las nuevas conexiones se podrá observar en la línea roja indicada en la imagen.



Costos

A continuación, en las siguientes tablas se presentarán valores aproximados que se requieren saber para poder cubrir lo necesario en caso de que se dañe la central telefónica existente.

Central Telefónica

La central telefónica será una Siemens Hipath 4000 que deberá cumplir con las mismas especificaciones y que reemplazará a la actual central telefónica dentro de la empresa.

Ítem	Descripción	Cantidad	Precio Unitario (US$)	Precio Total (US$)
1	Central Telefónica Hipath 4000 con mando duplex	1	34635,65	34635,65
		Total		34635,65

Licencias para puertos analógicos y digitales Hipath 4000

Ítem	Descripción	Cantidad	Precio Unitario (US$)	Precio Total (US$)
2	Licencias Flex para Hipath 4000	240	84,03	20167,2
		Total		20167,2

Especificaciones Técnicas

- Licencias Flex Licence para puertos analógicos y digitales Hipath 4000.

Licencias para usuarios IP Hipath 4000

Ítem	Descripción	Cantidad	Precio Unitario (US$)	Precio Total (US$)
3	Licencias de comScendo Hipath 4000	16	84,03	1344,48
		Total		1344,48

Especificaciones Técnicas

- Licencias comScendo para conectar teléfonos IP a Hipath 4000.

Módulos IP

Ítem	Descripción	Cantidad	Precio Unitario (USS)	Precio Total (USS)
4	Módulos IP	3	3077,23	9231,69
		Total		9231,69

Este tipo de productos son compatibles para la actual central telefónica.

Módulos de 2 enlaces digitales

Ítem	Descripción	Cantidad	Precio Unitario (USS)	Precio Total (USS)
5	Módulos de 2 enlaces digitales E1 PRI CCS DIUT2	2	1547,53	3095,06
		Total		3095,06

Este tipo de productos son compatibles para la actual central telefónica.

Agrupando todos los artículos anteriormente e incluyendo otros adicionales se especificaran en la siguiente tabla:

Ítem	Descripción	Cantidad	Precio Unitario (USS)	Precio Total (USS)
1	Central Telefónica Hipath 4000 con mando dúplex	1	34635,65	34635,65
2	Licencias Flex para Hipath 4000	240	84,03	20167,2
3	Licencias de comScendo Hipath 4000	16	84,03	1344,48
4	Módulos IP	3	3077,23	9231,69
5	Módulos de 2 enlaces digitales E1 PRI CCS DIUT2	2	1547,53	3095,06
6	Extensiones Análogas a/b	312	89,23	27839,76
7	Extensiones Digitales UPO/E	96	65,32	6270,72

8	Troncales Analógicas	72	80,35	5785,2
9	Troncales/Enlaces Digitales ISDN S0-S2 PRI	4	467	1868
10	Redundancia de mando	1	76543,23	76543,23
11	Módem de mantenimiento remoto 56kbps	1	1400	1400
12	Distribuidor principal (MDF)	1	8332	8332
13	Líneas de conmutación de emergencia (ALUM)	4	1320,12	82580,48
14	Rack dedicado de 19¨ para colocación fuente de poder	3	2001,54	6004,62
15	Gateway IP HG3530 V2.0 para Telefonía IP	5	6960	34800
16	SHP 380 G9	4	8900	35600
			Subtotal	355498,09
			Iva	42659,77
			Total	398157,86

- Para poder cubrir este tipo de vulnerabilidad necesitamos un **presupuesto total de 398 157.86 dólares** tanto en equipamiento como en servicios.
- Forma de Pago: Correspondiente con la actual empresa proveedora se la realizará con el 50% de anticipo y 50% contra entrega.
- Plazo de entrega: Entrega será inmediata previa a la verificación de stock.
- La validez de oferta: 30 días calendario contados a partir de su emisión.

A continuación se realizará un estudio del SLA, definición, beneficios, contenido, cláusulas, cómo funcionan y se manejan los sistemas de respaldo de la Hipath 4000 v2 de forma clara y sencilla.

Una vez estudiada la primera solución, podemos concluir que la instalación de una central espejo es una opción recomendable para cuando se dañe la actual central y no se caiga el sistema de telefonía. Es muy poco probable que una central telefónica llegue a dañarse y como hemos estudiado la HIPATH 4000 y adjuntando la información de las encuestas, esta se encuentra en buenas condiciones, por lo tanto, ya está cubierto este tipo de problema.

Finalmente, cuando nos referimos a la parte presupuestaria si sería otro problema para la empresa, para esto es muy importante realizar mantenimientos a los equipos y mucho mejor si se trabaja con una empresa proveedora.

Solución Dos: Service Level Agreement (SLA)

Un Service Level Agreement se considera un documento formal (contrato escrito) entre dos entidades que son: proveedor de servicios y cliente donde fijan acuerdos en la calidad de los servicios con el fin de dar soluciones a los problemas. Algunos términos que se pueden nombrar dentro de un SLA son: el tiempo de respuesta para resolver problemas, el personal encargado para el servicio, la documentación necesaria, las prioridades que se definen, garantías, responsabilidades, mediciones de servicio y la finalización de los servicios ofrecidos. (Rouse, Search IT Channel, 2015)

En este contrato se definen todas las necesidades que el cliente necesita dentro de su empresa o trabajo con el objetivo de simplificar cualquier problema que pueda producirse. Para ofrecer un buen SLA, una de las principales características que deberían tener es la garantía por parte del proveedor que va a soportar todo el trabajo generando niveles de calidad aceptables, la disponibilidad de horarios y el tiempo de respuesta. Una vez especificado todas las necesidades que el cliente ha dicho y llegando a un acuerdo con el proveedor contratado, se dará a conocer los costos del servicio.

Cuando se vaya a realizar el contrato escrito entre las dos partes siempre debe existir una persona encargada o responsable de parte del cliente al negociar con el proveedor. Esta persona estará encargada de dar seguimiento al proveedor para asegurarse que cumpla con todos los servicios que ofrece y en caso de percibirse algún percance se deberá realizar las penalizaciones correspondientes. Por lo tanto, dentro del contrato se indicará de manera muy clara los puntos a tratarse. (Rouse, Search IT Channel, 2015)

Una herramienta de mucha utilidad para definir y negociar un buen SLA tanto para clientes como para proveedores es el triángulo de variables como: los niveles de servicio, la flexibilidad del proveedor y el costo del servicio de tal manera que el cliente tome el control de una variable y el proveedor de las demás dándose tres combinaciones como:

1. Si el cliente quiere definir los niveles de servicios, entonces el proveedor deberá establecer qué tanta flexibilidad podrá tener y cuál será el costo. (Networld, 2002)

2. Si el cliente elige tener mucha flexibilidad, entonces el proveedor deberá establecer a qué niveles de servicio se puede comprometer y cuál sería el costo. (Networld, 2002)

3. Si el cliente elige definir el costo entonces el proveedor determinará la flexibilidad y los niveles de servicio. (Networld, 2002)

Contenidos de un SLA

El contenido de un SLA puede variar de acuerdo al tipo de servicio que se ofrece, por lo general, la principal información que abarca un SLA es la siguiente:

1. Nombre del servicio
2. Información de autorización (con fecha y lugar)
    a. Gestor del nivel de servicio
    b. Cliente
3. Duración del contrato
    a. Fechas de comienzo y final
    b. Reglas de terminación del contrato
4. Descripción y resultados deseados por el cliente
    a. Necesidades que el cliente necesita
5. Referencias a contratos adicionales
6. Tiempos de servicio
    a. Horarios disponibles del servicio
    b. Periodos de mantenimiento
    c. Excepciones(feriados y fines de semana)
7. Tipos y niveles de apoyo requeridos
8. Apoyo a distancia

9. Requisitos/metas de Nivel de servicio
    a. Metas disponibles
        i. Condiciones de disponibilidad de los servicios
        ii. Confiabilidad
        iii. Tiempos
        iv. Restricciones
        v. Requisitos
    b. Metas de capacidad/desempeño
        i. Tiempos de respuesta
        ii. Requisitos referentes a informes de desempeño
10. Estándares técnicos ordenados y especificaciones del servicio técnico
11. Responsabilidades
    a. Deberes del proveedor
    b. Deberes del cliente
    c. Responsabilidades de los usuarios
12. Costos y precios
    a. Costos de proveer el servicio
    b. Reglas por penalidades
13. Horarios de cambios

(itprocessMaps, 2013)

Cláusulas de un SLA

Algunas cláusulas que se pueden nombrar son las siguientes:

- Nivel específico del soporte a los clientes
- Opciones de soporte
- Especificaciones con el software y hardware que se otorga y su precio
- Definir, documentar, acordar, monitorear, medir, reportar y revisar el nivel de servicio provisto por IT.
- Mantener la relaciones de comunicación con el negocio y cliente
- Monitorear y mejorar la satisfacción del cliente.
- Asegurar que las partes involucradas estén de acuerdo con el servicio prestado
- Asegurar y mantener las respectivas medidas para mejorar la calidad del servicio.

Beneficios de obtener un SLA

- Mejorar el tiempo de actividad, la seguridad y el desempeño de los sistemas por medio de monitorizaciones periódicas que les permiten solucionar problemas antes que se ocurra un problema.
- Permite que los empleados trabajen más eficientemente disminuyendo su tiempo y esfuerzo en actividades extras.
- Mejora la productividad de los empleados y la capacidad de respuesta al cliente
- Optimiza la rentabilidad del negocio y ayuda a solucionarlo rápidamente en caso de un desastre.
- Se caracteriza por ser un proceso estructurado
- Hace referencia al mejoramiento continuo.
  (ASIR, 2015)

Alcance de requerimientos

- Objetivo de la Contratación

El objetivo de esta Contratación es proveer a la institución, el Servicio de Soporte en Sitio para Telefonía IP y Comunicaciones Unificadas , mediante el cual proveedor pondrá a disposición de la institución un número anual de 160 horas para ser utilizadas por la institución en la resolución de problemas, actualización de sistemas operativos y cambios de configuración en equipos de Telefonía IP y Comunicaciones Unificadas que se encuentren en producción, según los términos y condiciones que se establecen en este documento.

1. Beneficio del Servicio propuesto

El Servicio propuesto por el proveedor representa los siguientes beneficios para la institución:

a) Acceso al soporte directo del proveedor con niveles de escalamiento a los laboratorios del proveedor, asistencia telefónica y/o asistencia en sitio.
b) Acceso a consultas y soporte técnico a los especialistas de Telefonía IP para optimizar el rendimiento de la red de comunicaciones de la institución.

c) Talleres de trabajo sobre inquietudes o nuevas implementaciones de los productos.

2. Descripción del Servicio de Soporte Técnico

a) Alcance del Servicio

El Alcance del Servicio propuesto está definido por las siguientes actividades:

- ✓ El proveedor pondrá a disposición de la institución números telefónicos y cuentas de correo electrónico, a las cuales reportar los informes de problemas y/o requerimientos.

- ✓ El proveedor deberá recibir los Informes de Problemas dentro del Horario Básico de Soporte (08:30 – 17:30).

- ✓ El proveedor pondrá a disposición de la institución de ciento sesenta (160) horas/hombre anuales de Servicios para Telefonía IP y Comunicación Unificadas que deberán ser utilizadas en actividades de resolución de problemas, actualización de sistemas operativos y cambios de configuración en la plataforma actual que se encuentran en producción, durante el Horario Básico de Soporte.

- ✓ El proveedor también proveerá horas/hombre de soporte fuera del Horario Básico de Soporte. Cada hora/hombre de soporte en sitio que se preste fuera del Horario Básico será contabilizada como hora y media (1.5) de soporte empleada por la institución.

- ✓ Los soportes en sitio se contabilizarán como dos (2) horas para las primeras dos (2) horas o fracción, a partir de la tercera hora se contabilizará cada hora o fracción como una (1) hora.

- ✓ Los soportes telefónicos se contabilizarán como una (1) hora por cada hora o fracción utilizada.

- ✓ El Servicio Técnico será prestado sin cargos adicionales por movilizaciones, siempre que el mismo sea ejecutado en un radio de veinte (20) kilómetros alrededor de la ciudad de Quito.

Las horas/hombre para los Servicios especificados en este documento podrán ser empleadas, a solicitud de la institución, o ante una sugerencia del proveedor.

Costos del SLA

Servicios	Descripción	Cantidad
1	Servicios de instalación, configuración, pruebas y capacitación	13661,82
2	Servicios de soporte especializado, mantenimiento preventivo y provisión de respuestas	18647
	Subtotal	32308,82
	Iva	3877,06
	Total	36185,88

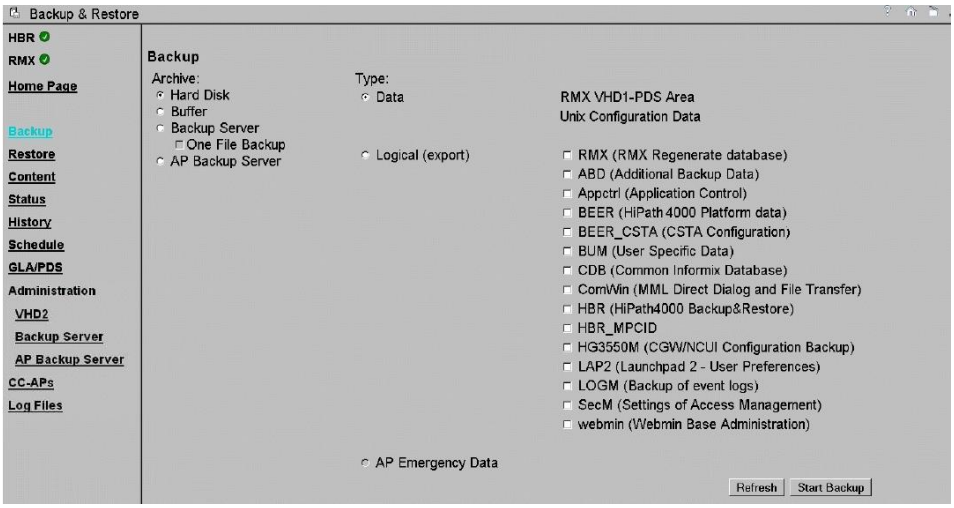
El costo aproximado anual de un contrato con este tipo de características que incluye servicios de instalación, configuraciones, pruebas, servicios de soporte y mantenimiento preventivo es de **434 230,56 dólares**

Solución Tres: Manejo de Sistemas de Respaldo

Sistema de Respaldo

El sistema de Backup y Restore viene como un componente de la HiPath 4000 donde guarda los datos de configuración o software de aplicaciones en un archivo de copia de seguridad y restaura los datos a petición. Backup y Restore por lo tanto se asegura de que una copia de seguridad precisa de los datos y/o software estará disponible en caso de un fallo del sistema. (Unify, 2013)

Las copias de seguridad del sistemas de puede hacer por unidades específicas o copias de seguridad de todo el sistema. Existen algunas tipos de copia de seguridad como:



- Copias de seguridad de Disco
    - Datos almacenados de tipo datos
    - Datos almacenados de tipo lógico
    - Datos almacenados automáticamente de tipo datos

Se puede realizar hasta 10 sets automáticos de copia de seguridad, los primeros datos almacenados de forma automática no se pueden sobre escribir. (Unify, 2013)

- Copias de seguridad de tipo TAPE – DAT
    - Datos almacenados de tipo datos
    - Datos almacenados de tipo lógico
    - Datos almacenados automáticamente de tipo datos

No permite más de un set de copia de seguridad. Un nuevo grupo de respaldo sobrescribe un conjunto de copia de seguridad, posiblemente existente, incluso si el nuevo conjunto de copia de seguridad es de un tipo diferente. (Unify, 2013)

- Copias de seguridad del Servidor
    - Datos almacenados de tipo datos
    - Datos almacenados de tipo lógico
    - Datos almacenados automáticamente de tipo datos

    Se permite hasta un grupo máximo de 4 respaldos

- Copias de Seguridad de Buffer

- Datos almacenados de tipo datos
- Datos almacenados de tipo lógico
- Datos almacenados automáticamente de tipo datos

No se permite más de 1 copia de seguridad. Un nuevo grupo de respaldos sobrescribe un conjunto de copia de seguridad, posiblemente existente, incluso si el nuevo conjunto de copias de seguridad es de un tipo diferente. (Unify, 2013)

Copia de seguridad del tipo "Datos"

Se considera una copia de seguridad de los datos que pueden contener las siguientes unidades

- UNIX_CFDATA
- BEER
- BEER_CSTA
- HG3550M
- RMX

Copia de Seguridad del tipo "Lógico"

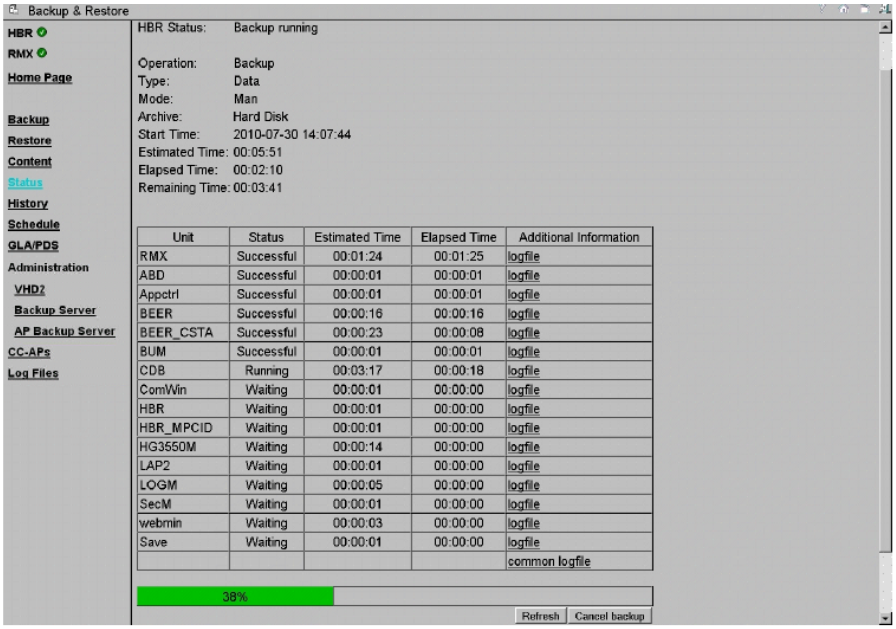
Un conjunto de copia de seguridad del tipo lógico se utiliza para importar o exportar datos de su elección (ejemplo: base de datos). Copia de seguridad lógica / restauración de datos se ejecuta en unidades. Una unidad consta de un grupo de aplicaciones interconectadas. La aplicación se utiliza para referirse a un paquete instalado software o varias partes de diferentes paquetes que han sido instalados.

Una nueva copia de seguridad sobrescribe un conjunto de copia de seguridad ya está archivada del mismo tipo en un archivo. Conjuntos de copias de seguridad de los diferentes tipos pueden ser almacenados juntos en el mismo archivo a excepción de cinta y búfer de E / S. (Unify, 2013)

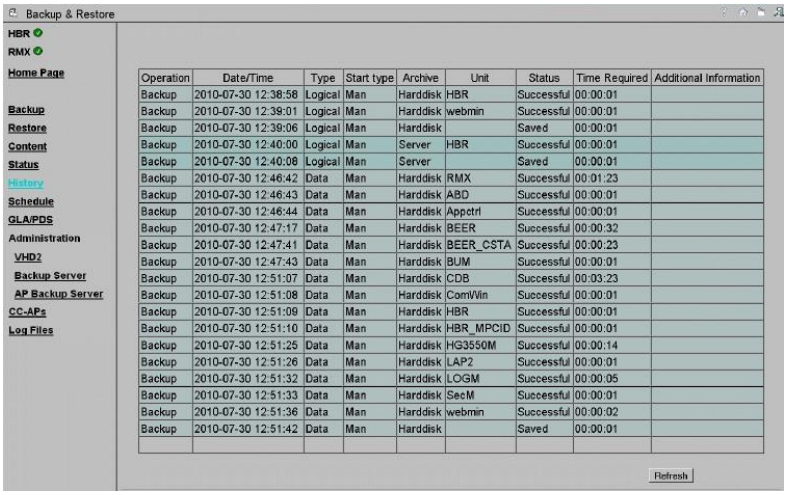
Una copia de seguridad manual se inicia con el botón Iniciar copia de seguridad en el cuadro de diálogo Copia de seguridad.

Posteriormente el estado de la copia de seguridad por ciclo actualmente en ejecución o del último en ser ejecutada se muestra en la pantalla de estado. La información mostrada incluye el estado general de HBR, el estado de copia de seguridad / restauración de las operaciones actualmente en ejecución y copia de seguridad anterior / operaciones de restauración. (Unify, 2013)

La pantalla se actualiza automáticamente cada 20 segundos.

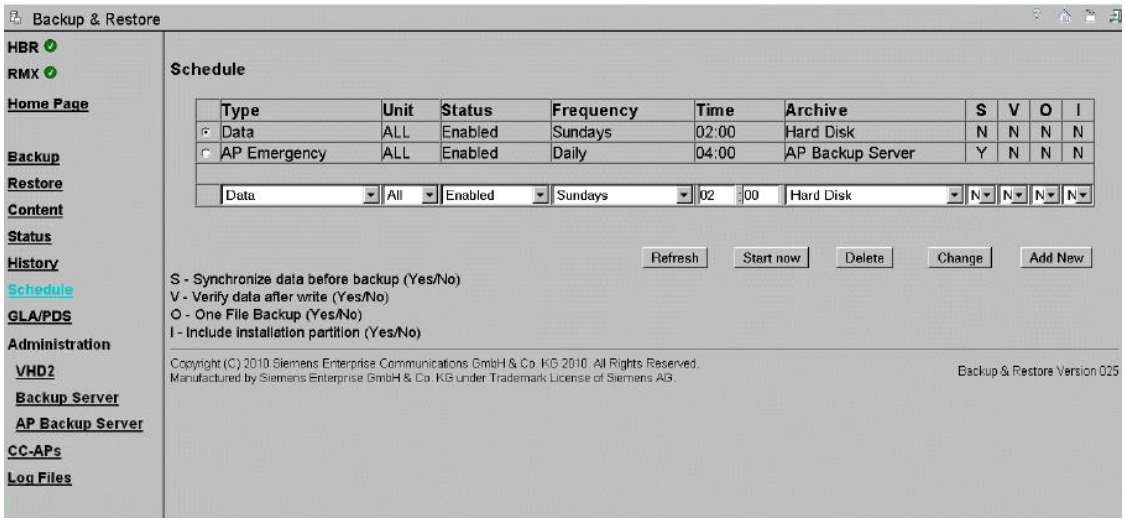


En la opción Historia, se mostrará una lista de estado de la última copia de seguridad de las operaciones que se llevarán a cabo se muestra en la pantalla Historia / restauración. Hasta la 25 de copia de seguridad / restaurar los ciclos se pueden mostrar.



Operation	Date/Time	Type	Start type	Archive	Unit	Status	Time Required	Additional Information
Backup	2010-07-30 12:36:58	Logical	Man	Harddisk	HBR	Successful	00:00:01	
Backup	2010-07-30 12:39:01	Logical	Man	Harddisk	webmin	Successful	00:00:01	
Backup	2010-07-30 12:39:06	Logical	Man	Harddisk		Saved	00:00:01	
Backup	2010-07-30 12:40:00	Logical	Man	Server	HBR	Successful	00:00:01	
Backup	2010-07-30 12:40:08	Logical	Man	Server		Saved	00:00:01	
Backup	2010-07-30 12:46:42	Data	Man	Harddisk	RMX	Successful	00:01:23	
Backup	2010-07-30 12:46:43	Data	Man	Harddisk	ABD	Successful	00:00:01	
Backup	2010-07-30 12:46:44	Data	Man	Harddisk	Appctrl	Successful	00:00:01	
Backup	2010-07-30 12:47:17	Data	Man	Harddisk	BEER	Successful	00:00:32	
Backup	2010-07-30 12:47:41	Data	Man	Harddisk	BEER_CSTA	Successful	00:00:23	
Backup	2010-07-30 12:47:43	Data	Man	Harddisk	BUM	Successful	00:00:01	
Backup	2010-07-30 12:51:07	Data	Man	Harddisk	CDB	Successful	00:03:23	
Backup	2010-07-30 12:51:08	Data	Man	Harddisk	ComVin	Successful	00:00:01	
Backup	2010-07-30 12:51:09	Data	Man	Harddisk	HBR	Successful	00:00:01	
Backup	2010-07-30 12:51:10	Data	Man	Harddisk	HBR_MPCID	Successful	00:00:01	
Backup	2010-07-30 12:51:25	Data	Man	Harddisk	HG3550M	Successful	00:00:14	
Backup	2010-07-30 12:51:26	Data	Man	Harddisk	LAP2	Successful	00:00:01	
Backup	2010-07-30 12:51:32	Data	Man	Harddisk	LOGM	Successful	00:00:05	
Backup	2010-07-30 12:51:33	Data	Man	Harddisk	SecM	Successful	00:00:01	
Backup	2010-07-30 12:51:36	Data	Man	Harddisk	webmin	Successful	00:00:02	
Backup	2010-07-30 12:51:42	Data	Man	Harddisk		Saved	00:00:01	

Para que se pueda introducir los datos durante varios ciclos de copia de seguridad automatizada en el cuadro de diálogo Programación. Puede definir cuándo y con qué frecuencia se debe ejecutar un ciclo de copia de seguridad automática. Para ello, las nuevas funciones se han proporcionado para añadir, modificar y borrar entradas.



	Type	Unit	Status	Frequency	Time	Archive	S	V	O	I
◉	Data	ALL	Enabled	Sundays	02:00	Hard Disk	N	N	N	N
○	AP Emergency	ALL	Enabled	Daily	04:00	AP Backup Server	Y	N	N	N
	Data	All	Enabled	Sundays	02 : 00	Hard Disk	N	N	N	N

En el cuadro de diálogo se especifica lo siguiente:

- Tipo (type): Datos o Lógicos
- Unidad (Unit): Todo los componentes del software (aplicaciones) instaladas en el sistema y copias de seguridad importantes
- Frecuencia (frecuency): Diario, Semanal, Mensual, Anual
- Tiempo (time): hora
- Archive (archivos): todos los tipos de backup disponibles
- Sincronización (S): SI/NO
- Verificación de trasferencia de datos (V): SI/NO

- Copia de seguridad de un archivo (O): SI/NO
- Incluya partición de instalación (I): SI/NO

Sistema de Alimentación

La central telefónica cuenta con sistemas de alimentación como: sistema de corriente alterna (redundante y no redundante) y sistema de corriente continua, sólo redundante. Dentro de la empresa, ésta central está configurada en modelo Dúplex, es decir, dispone de dos controles centrales (CC) y un procesador de servicios y datos. Cada módulo CC se alimenta con alimentación propia. El procesador de administración y datos (ADP) se alimenta a través de dos módulos de alimentación separados, lo que hace que esté listo para el servicio e incluso si falla la alimentación de corriente.

En el modelo Dúplex la tarjeta DSCXL que es el módulo de procesamiento central y responsable de las funciones principales del control de sistema, puede funcionar como mando central o como tarjeta de administración del equipo (ADS) encargado de controlar los buses del panel posterior del equipo y sus respectivas funciones.
(Manual Técino Siemens HIPATH, 2007)

Sistema de Backup de Archivos KDS (Memoria de los datos del Cliente)

Guardar los archivos KDS

La memoria de los datos del cliente recogen todos los ajustes individuales del sistema de comunicación. Para poder realizar cualquier configuración de estos archivos KDS se deberá usar la aplicación HiPath 4000 Manager. Si se requiere guardar estos archivos KDS es recomendable transferirlos primero, de tal forma quedará garantizado que los datos a editar correspondan a la versión más actual reciente y por motivos de seguridad, se deberán almacenar en un portador de datos.

Los archivos KDS se guardan con el formato *.kds, si se lo hace por primera vez aparecerá un cuadro de diálogo donde se indicará escribir el nombre con el que se desea guardarlo. Como sugerencia se dice que una vez guardadas estos archivos ya sea de forma manual o automática, no se podrán usar el modo Delta para transferir la base de datos desde el PC al sistema de comunicación ya que no se transferirán los datos más actuales. Por defecto al guardar estos archivos recibirá el nombre de **lastload.kds.** (Manual Técino Siemens HIPATH, 2007)

Copia de seguridad de KDS de forma manual

La copia de seguridad de forma manual de los archivos KDS se los puede realizar por medio de las herramientas Manager E o Manager T (herramienta basada en MS Windows para la administración del sistema de todos los datos relativos al servicio técnico y al cliente por parte del servicio técnico). La reposición de los archivos KDS a partir de la tarjeta MMC, incluyendo los datos de tarificación que puede activarse asimismo manualmente. (Manual Técino Siemens HIPATH, 2007)

En este cuadro indicamos paso a paso el proceso para la copia de seguridad.

Pasos	Proceso
Protección manual de los datos de cliente en la tarjeta MMC	
1	Iniciar la administración del sistema
2	Procesar KDS
3	Almacenar datos de KDS
4	Almacenar KDS en la tarjeta MMC
Carga de los KDS en la tarjeta MMC al sistema	
1	Iniciar administración del sistema
2	Procesar KDS
3	Almacenar datos KDS
4	Almacenar KDS de la tarjeta MMC, al finalizar se reiniciara el sistema

Copia de seguridad de KDS con HiPath Software Manager

Las copias de seguridad de los archivos KDS se depositan en un directorio que debe especificarse previamente. Esta copia de datos debe identificarse de forma manual inmediatamente o realizarse a una hora preseleccionada o de forma.

Por medio del módulo HiPath Software Manager permite realizar copias de seguridad de los componentes del sistema y base de datos. Si se requiere realizar un backup total, se guardarán los datos de todos los sistemas que se encuentren en la red, dando la posibilidad de proteger los datos del sistema determinados o de todo el sistema.

Si se requiere un backup de las base de datos, se podrá visualizar un esquema general de todas las bases de datos (Feature Server, SQL Server). También existe la posibilidad de proteger los datos de una o de todas las bases de datos. (Manual Técino Siemens HIPATH, 2007)

Tratamiento de los KDS al sustituir el hardware central

En el caso de que exista un defecto en el hardware, es necesario sustituir un módulo de control central sujeto a licencias y deberá solicitarse siempre un archivo de licencia nuevo. Como consecuencia de la sustitución se modificara la dirección MAC. (Manual Técino Siemens HIPATH, 2007)

Por lo tanto el siguiente procedimiento para realizar la carga de los KDS actuales es el siguiente:

Pasos	Acción
1	Realizar un volcado de la KDS actual y almacenarla en la tarjeta MMC
2	Desconectar el sistema de la corriente.
3	Extraer la tarjeta MMC
4	Reemplazar el módulo de control central.
5	Insertar la MMC.
6	Volver a conectar el sistema enchufando el conector de red.
7	La KDS almacenada anteriormente en la MMC se carga de nuevo en la RAM del sistema. De esta forma queda configurado el sistema del cliente: • Los terminales inalámbricos CMI están dados de alta. • La velocidad binaria V.24 está ajustada. • El puerto de login ACD está configurado. • Todos los ajustes de los terminales, tales como volumen y ajustes del display, están configurados para cada extensión.

Proceso para cargar los KDS antiguos:

Pasos	Acción
1	Almacenar KDS actuales con la HiPath 4000
2	Desconectar el sistema de la corriente.
3	Extraer la tarjeta MMC.
4	Reemplazar el módulo de control central.
5	Insertar la MMC

6	Volver a conectar el sistema enchufando el conector de red.
7	Realizar un reload
8	Si se desea utilizar un estado de la KDS “más antiguo”, la KDS debe cargarse en el sistema.
9	Realizar un reset. De esta forma que queda configurado el sistema del cliente. A continuación hay que ● Dar de alta de nuevo los terminales inalámbricos CMI. ● Ajustar de nuevo la velocidad binaria V.24. ● Volver a configurar el puerto de login ACD. ● Volver a configurar los ajustes de los terminales

5.1.2 Vulnerabilidad 2: Falta de Sistema de Calidad de Servicio (QoS)

Una segunda vulnerabilidad encontrada dentro de la empresa CELEC EP TRANSELECTRIC gracias a los resultados de la encuestas, es la falta de disponibilidad de un sistemas de calidad de servicio, esto se puede evidenciar dentro de la mismas encuestas ya que los empleados tienen que lidiar con diferentes problemas en el servicio de telefonía como: problemas de eco, problemas en sus llamadas, fallas en las conversaciones. Esto se puedo evidenciar ya que los porcentajes en los resultados son importantes.

Para esto una de mis propuestas es que implementen un servicio de calidad (QoS) más adecuado dentro del edificio principal de CELEC EP TRANSELECTRIC.

Por lo tanto, tendremos que estudiar los diferentes tipos de calidad de servicios que existen, conocer su definición, su funcionamiento y beneficios.

5.1.2.1 Tipos de QoS

Cuando hablamos de calidad de servicio estamos nombrando a tres tipos de QoS que se utilizan y son:

- IntServ (Servicios Integrados)
- DiffServ (Servicios Diferenciados)

5.1.2.1.1 Servicios Integrados (IntServ)

Se considera un tipo de sistema de calidad de servicio que proporciona un servicio garantizado de los paquetes a través de reservas de paquetes que pasan por cada nodo.

IntServ trabaja con el protocolo RSVP (Resource Reservation Protocol) que es el encargado de realizar las reservaciones de los recursos y del mantenimiento de la red de cada flujo, si la red llega a congestionarse entre protocolo se encargará de proporcionar ciertas características de QoS.

Este sistema de calidad de servicio no es un modelo de escalabilidad ya que tiene recursos limitados. Otro problema es su alto costo en el manejo, de sus políticas y equipos que soporten este tipo de QoS. Tanto RSVP e IntServ trabajan juntos para dar acceso a la red donde existen enlaces de baja capacidad y los equipos como routers soportan pocos flujos.

Protocolo RSVP

El protocolo RSVP se considera un protocolo de señalización de QoS dentro de IntServ que permite establecer reservas de recursos limitados. Este protocolo controla los envíos de paquetes de datos entre el emisor y el receptor o la conexión entre los diferentes nodos o routers aplicando ciertas políticas de QoS.

Cuando el emisor utiliza RSVP reserva recursos durante todo el camino hacia el receptor, esta reserva funciona si entre los nodos por donde pasan los paquetes existe prioridad de paquetes y también la confirmación del solicitante. Si el router no dispone de suficientes recursos para garantizar el QoS, se descarta el flujo, por lo tanto el RSVP se encarga de las reservas.
(BidDigital, 2015)

Características de RSVP

- Capaz de reservar cierto ancho de banda para cada nodo y cada flujo.
- Capaz de transformar y mantener ciertos parámetros y políticas de QoS.
- Los recursos están garantizados.
- La reservas con realizadas en una sola dirección, si se desea que sea bidireccional debe ser hecha por cada extremos. (DanySoft, 2013)

Cuando hablamos de la arquitectura de IntServ decimos que lo flujos son unidireccionales y pueden ser agrupados por clases dando la misma calidad de servicio a cada uno. Se pueden nombrar tres tipos de servicios como: (Montañana, 2013)

- Servicio garantizado
- Servicio de carga controlada
- Servicio de Best Effort

Servicio Garantizado

Este servicio ofrece calidad de voz garantizada ya que entrega un determinado ancho de banda. Garantiza que los paquetes de datos lleguen dentro del tiempo establecido y que no serán descartados si se congestiona la red, siempre y cuando la congestión de la red o el tráfico de flujo este controlado.

Servicio de Carga Controlada

El servicio provee a los clientes flujos de QoS iguales al QoS que el mismo flujo recibirá en un elemento de la red y asegurar que el servicio sea recibido. Este servicio en similar al Best Effort, ofrece un buen tiempo de respuesta, el flujo no se deteriora, los routers no proporcionan garantías estrictas y pueden producir retardos grandes. (Peñafiel, 2005)

Arquitectura de los Servicios Integrados

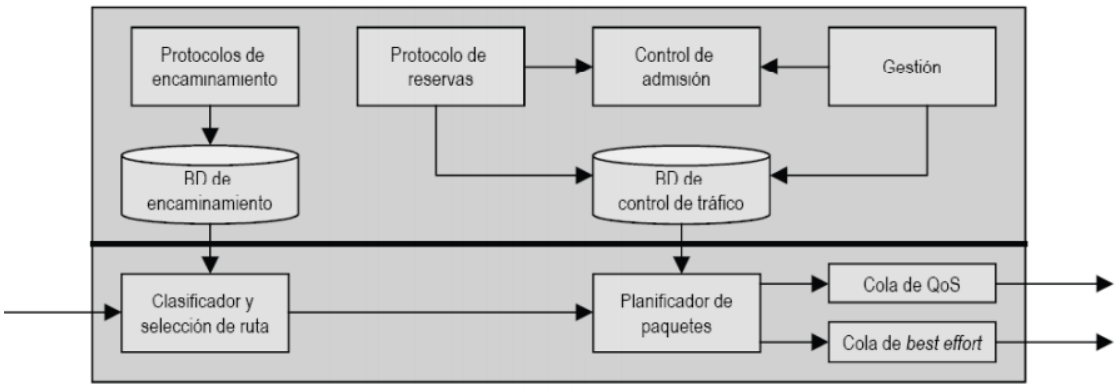


Figura 5.1.2.1 Arquitectura IntServ

(Ternero, 2010)

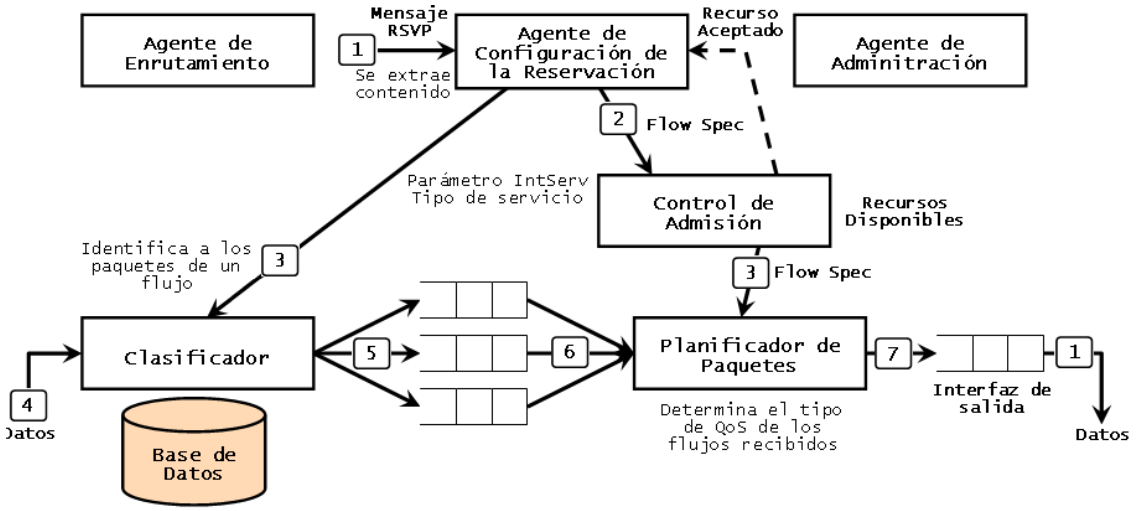


Figura 5.1.2.2Arquitectura IntServ

(Alvarez, 2007)

Protocolo o Agente de enrutamiento: Maneja la base de datos de enrutamiento, donde se especifica el siguiente salto e implementan un protocolo particular para el enrutamiento.

Protocolo de Reservas o Agente de la configuración de la reservación: Es el encargado de realizar las reservas de recursos para los flujos por medio del protocolo RSVP, que se puede dar entre routers.

SI en el control de admisión acepta una nueva petición, dichos cambios se realizan en la base de datos del planificador de paquetes y en el clasificador. (Martinez)

El Flow Spec describe para quienes es la reservación y envía la información a cada router de su trayectoria mediante el RSVP

Control de Admisión: Es el encargado de determinar si aún existen recursos suficientes, para cada flujo nuevo. (Martinez)

Agente de Gestión o Administración: Encargado de establecer las políticas de control de admisión como monitoreos y medir los recursos disponibles, determinar si a un nuevo flujo se le puede otorgar calidad de servicio. (Martinez)

Clasificador y selección de ruta: Cada paquetes se coloca en colas individuales, los paquetes se clasifican en clases, las clases se determinan en función de algunos

campos de la cabecera IP y finalmente se realiza el siguiente salto de acuerdo a la clase del paquete e IP destino. (Martinez)

Dentro del clasificador de paquetes y del planificador de paquetes se revisan la dirección IP, identificación del protocolo, puerto de origen y puerto de destino para clasificarlos y ponerlos en sus respetivas colas.

Planificador de paquetes o gestor de cola de paquetes: Es el encargado de ordenar y transmitir los paquetes en base a su clase y base de datos del control de tráfico determinando el tipo de QoS de los flujos recibidos y políticas de vigilancia. (Martinez)

5.1.2.1.2 Servicios Diferenciados (Diffserv)

Los sistemas diferenciados son considerados otro sistema de calidad de servicio que ofrece calidad a través de clases. La mayoría de la redes de basan en los DiffServ, este modelo identifica las comunicaciones según el paquete, para cada paquete la red analiza una seria de campos y de acuerdo al valor aplicará características de prioridad, ancho de banda y dará cierto QoS. (Redes Convergentes: Internet de las cosas, 2014)

Dentro de la cabecera de cada paquete se encontrará un campo llamado TOS (tipo de servicio), el cuál identificará el tipo de clase al que pertenecerá. Los routers son los encargados de tratar a cada paquete según su categoría y no guardan información sobre el estado de los flujos.

Para poder obtener este tipo de QoS se necesita tener un contrato entre el cliente y el proveedor el cuál garantizará la QoS a cada paquete.

El objetivo de los sistemas diferenciados es proporcionar un ancho de banda de la red hacia los diferentes usuarios de forma equitativa y controlada de tal manera que pueden realizar aplicaciones de audio y video, transferencias de archivos, entre otras sin ningún inconveniente

Características

- No existe reservación de recursos de flujo como en los sistemas integrados (IntServ).

- Garantiza los recursos asignados a cada servicio.

- Los paquetes son clasificados en la entrada de la red según el tipo de clase asignada y su prioridad respectiva.

- Mediante un contrato se especifica qué tipo de garantías se ofrece a cada clase y cuantas deberán ser enviadas dando un QoS determinado.

- El DSCP (Punto de código de Servicio Diferenciado) es el sector donde se marcaran los paquetes para realizar su salto.

Arquitectura Sistemas Diferenciados (DiffServ)

Dominio DS

El dominio DS se considera un conjunto de nodos que están conectados entre sí y proporcionan ciertas políticas de servicio de calidad usando los valores del DSCP y un conjunto de grupos denominados PBH (Per Hob Behavior).

PBH son los que determinan el tratamiento de los paquetes salto a salto en la red implementada en cada nodo. De acuerdo al grupo PBH y al valor DSCP del campo DS de la cabecera IP, se determina como se recibe los paquetes en cada nodo y se asigna su respectiva prioridad, es decir, cuando un paquete entra al router, el ruteo identifica el valor DSCP y el puerto de salida para finalmente mandar al paquete al tipo de cola específico.

El dominio DS está conformado por dos tipos de nodos: de frontera (entrada y salida) e interiores o núcleo.

Tipos de nodos

Nodos frontera: Son los encargados de clasificar a los paquetes basándose en los valores de la cabecera IP (dirección origen, dirección destino, identificador de protocolo) y posteriormente se los marca identificando a la clase que pertenecen. (Martinez)

Nodos Interiores: Son los encargados de reenviar los paquetes a través de recursos por clases, los nodos interiores están conectados a los nodos frontera siempre y cuando estos pertenezcan al mismo dominio DS. Gestionan el tráfico por clases de los paquetes

basados en el campo DS. Estos nodos funcionan junto con el PBH para el tratamiento de reenvío. (Martinez)

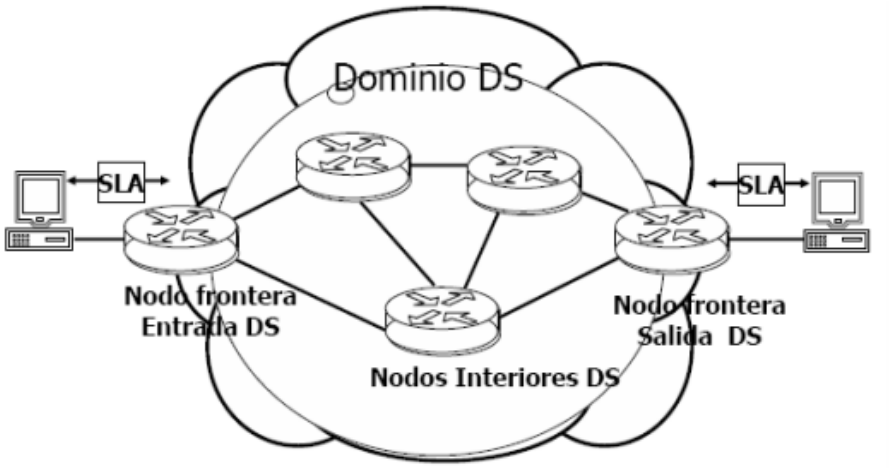


Figura 5.1.2.3 Ejemplo Dominio DS

(Martinez)

Campos TOS (Tipo de servicio)

Dentro de la cabecera IPv4, estudiaremos el campo TOS de 8 bits

Formato de la Cabecera IP (Versión 4)

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

Figura 5.1.2.4 Ejemplo Cabecera IPv4

(Luz, 2012)

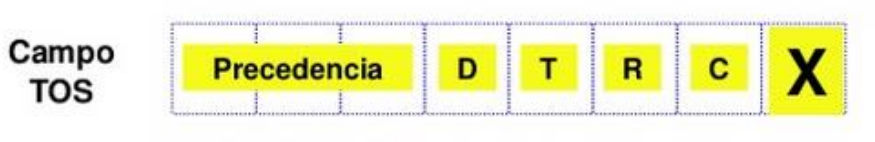


Figura 5.1.2.5 Campo TOS

(Salinas)

Dentro del campo TOS antes de aplicar el DiffServ, los 3 primeros bits, indican la precedencia IP, es decir, indica la prioridad de los paquetes y se los diferencia por medios de 8 tipos de clases.

Clase	Tipo de Precedencia
000	Rutina
001	Prioridad
010	Inmediato
011	Urgente
100	Muy urgente
101	Crítico
110	Control de encaminamiento
111	Control red

Tabla 5.1.2.1 Campo TOS-Precedencias

Los siguientes bits indicarán lo que se requiere utilizar en la ruta

D	1000	Mínimo retardo (delay)
T	**0100**	Máximo rendimiento (throughput)
R	**0010**	Máxima fiabilidad (reliability)
C	**0001**	Mínimo costo (cost)
X	**0000**	Bit reservado

Tabla 5.1.2.2 Campo TOS - Retardos Mínimos

Por lo tanto, una vez aplicado los servicios diferenciados al campo TOS se lo llamará campo DS y dentro de este campo se realizara la respectiva distribución de bits de la siguiente manera:

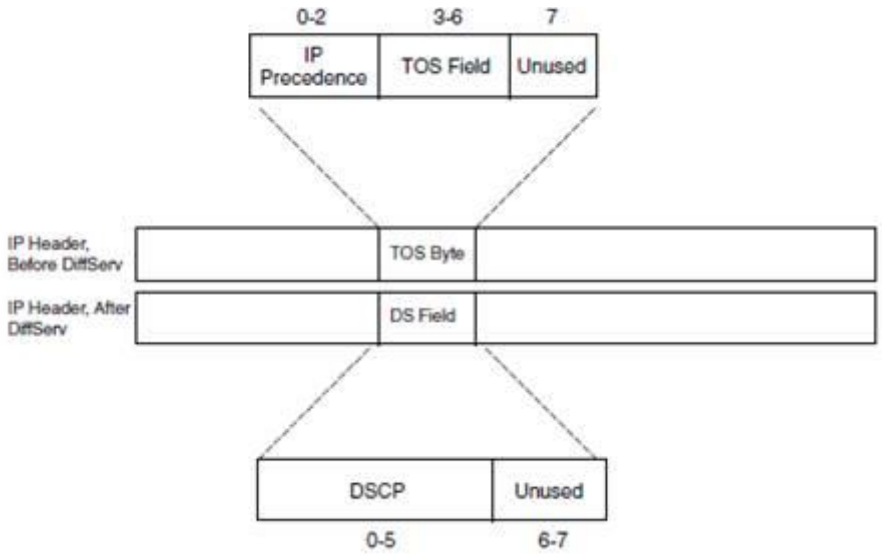


Figura 5.1.2.6 Campo TOS - DiffServ

(Estudio de priorización de tráfico para VoIP, 2013)

Figura 5.1.2.7 Campo DS

(Salinas)

- **Campos DSCP:** 6 primeros bits, punto de código de servicios diferenciados (Differentiated Service CodePoint DSCP), estos 6 bits indican el tratamiento que debe recibir el paquete en los routers , indica la prioridad del paquete.

- **CU:** código no utilizado (Currently Unused)

  Dentro del campo DSCP, la distribución de los bits es el siguiente:

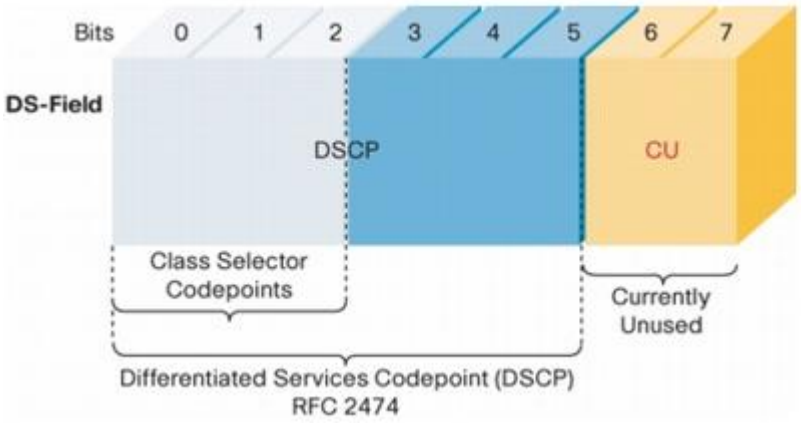


Figura 5.1.2.8 Campo DSCP - DiffServ

(Wikipedia, 2012)

- Los 3 primeros bits (0-2) son considerados para las clases de tráfico a las que pertenecen los paquetes, de igual forma clasificar en 8 clases y está definido como Codepoints Class Selector.
- Los 3 bits (3-6) se los utiliza como probabilidad de descarte.

Tipos de PBH

PBH Selector de clases (CS-Class Selector)

El PBH CS utiliza los campos de la precedencia IP para poder marcar la prioridad del tráfico en la red, donde está estructurado de la siguiente forma: “xxx000” comenzando con los valores “000000” de CS0 de prioridad más baja hasta CS7 con valores de “111000” con la prioridad más alta, donde x puede ser 0 ó 1. Este tipo de PBH usa Best Effort con prioridad, es decir, mientras más grande sea el tráfico, mejor QoS de proporcionará. (Calidade servicios (QoS), 2014) (Delfino & Rivero)

Precedencia IP	Nombre (DSCP CS)	Valores (DSCP CS)
000	**CS0**	**000**000
001	**CS1**	**001**000
010	**CS2**	**010**000
011	**CS3**	**011**000
100	**CS4**	**100**000
101	**CS5**	**101**000
110	**CS6**	**110**000
111	**CS7**	**111**000

Tabla 5.1.2.3 Precedencia IP - Valores DSCP CS

PBH Assured Forwarding Behavior (AF)

Este servicio de renvío asegurado está compuesto por tres tipos de descarte (prioridades), cuatro clases y a cada clase se puede asignar cantidad de recursos en los routers como es el ancho de banda, el espacio en los buffers, entre otras. (Delfino & Rivero)

Los tres primeros bits indica la clase a la que pertenece, a cada clase se la definen tres categorías de descarte de paquetes indicado en los tres siguientes bits del DSCP. Este servicio funciona cuando la red está congestionada y generalmente siempre se dará a los de prioridad más alta para ser descartado.

Por lo tanto existen 12 valores de DSCP que son:

Clase menos prioritaria

		DSCP	Prioridad de descarte de tráfico
Clase 1	AF11	**001** 010	Baja
	AF12	**001** 010	Media
	AF13	**001** 100	Alta
Clase 2	AF21	**010** 010	Baja
	AF22	**010** 100	Media
	AF23	**010** 110	Alta
Clase 3	AF31	**011** 110	Baja
	AF32	**011** 110	Media
	AF33	**011** 110	Alta
Clase 4	AF41	**100** 110	Baja
	AF42	**100** 110	Media
	AF43	**100** 110	Alta

Clase más prioritaria

Tabla 5.1.2.4 Prioridades de Descarte

(Arquitectura de Calidad de Servicios DiffServ e IntServ, 2012)

PBH por defecto (Default Forwarding)

Este servicio se denomina por defecto debido a que no hay prioridades, es decir, el tráfico no cumple con los requisitos de las clases por lo tant,o no hay garantías. El punto de código (codepoint) del DSCP es el “000000”. (Delfino & Rivero)

PBH reenvío acelerado (Expedited Forwarding - EF)

El comportamiento PBH EF garantiza que los paquetes reciban el mejor trato al enviarse por la red. Los paquetes tienen un trato preferencial por los enrutadores del modelo Diffserv que se encuentran hasta el destino del paquete.

Este servicio se considera el de mayor calidad ofreciendo garantías de bajo retardo, baja pérdida de paquetes, es perfecto para la voz, video y otros servicios en tiempo real. Su punto de código es “101110”. (Delfino & Rivero)

En esta tabla podemos apreciar un resumen de todos los valores de cada servicio:

DSCP	Binario
Predeterminado	000000
CS1	001000
AF11	001010
AF12	001100
AF13	001110
CS2	010000
AF21	010010
AF22	010100
AF23	010110
CS3	011000
AF31	011010
AF32	011 100
AF33	011110
CS4	100000
AF41	100010
AF42	100100
AF43	100110

CS5	101000
EF	101110
CS6	110000
CS7	111000

Tabla 5.1.2.5 Valores PBH

(Data Network Resource, s.f.)

Comparación de modelos IntServ vs DiffServ

1. IntServ no se considera un modelo escalable ya que cada router debe mantener el estado de los flujos.

2. DiffServ es un modelo escalable ya que los routers intermedios no necesitan mantener información de estado de los flujos gracias a su clasificación por clases y encolamientos.
   (Arquitectura de Calidad de Servicios DiffServ e IntServ, 2012)

3. Actualmente muchos proveedores ofrecen el servicio DiffServ en las empresas ya que algunos routers ya vienen implementadas este tipo de versiones.

4. La QoS en los DiffServ de basa en su dominio mientras que el IntServ se basa entre origen y destino. (Martinez)

5. Los dos servicios mantienen calidad de servicio, con la diferencia que en los DiffServ ofrecen garantías relativas y en los IntServ ofrecen garantías por flujo.

6. En los DiffServ los servicios se los realiza por separación de clases y prioridades mientras que los IntServ la separación se hace por flujo ya que necesita mantener las reservas.

7. En DiffServ los paquetes se clasifican por categorías para los saltos, mientras que IntServ necesita previas reservas para los diferentes saltos.

8. DiffServ se considera uno de los servicios más actuales y beneficiosos por lo que las empresas proveedoras optan por usar más ente servicio. (Martinez)

Planificación de las políticas de QoS

Para la correcta implementación de calidad de servicio debemos planificar sus políticas de calidad donde se debe revisar, clasificar y priorizar los servicios que proporciona la red, tomando en cuenta el ancho de banda disponible y determinar el porcentaje o tasa que se debe asignar a cada clase que se transfiere a través de la red.
Para esto debemos tomar en cuenta el siguiente proceso para la planificación de las políticas de QoS.

1. **Distribución de la red para QoS**

La distribución de la red se basa en la identificación de los enrutadores y host de la red con la que se va a trabajar para proporcionar los servicios diferenciados y que deberán ser compatibles con QoS.

Para esto se debemos seguir una serie pasos generales que se deben realizarse antes de crear las políticas de QoS y son los siguientes:

- Revisamos la distribución de la red, planificando una estrategia y usando los equipos disponibles.

- Identificamos los equipos para la distribución de la red y que sean capaces de soportar QoS.

- Determinamos en que equipos se aplicará las políticas de QoS.

- Revisamos cualquier tarea o configuración que se requiera por parte de los enrutadores para aplicar Diffserv

2. **Definición de clases**

Definimos las clases donde los servicios de la red van a ser divididos, en ciertos casos identificaremos la existencia de Vlan tanto para voz como para datos, así se proporcionará mayor prioridad a la voz.

Posteriormente las clases se definirán de la siguiente manera:

- Organizamos los flujos de tráfico en clases. Para una arquitectura Diffserv no se recomienda crear una clase por cada tipo de tráfico.

  Para esto se debe crear una tabla de planificación de QoS para organizar las políticas de QoS que van a ser necesarias. La estructura de la tabla es la siguiente:

Clase	Prioridad	Filtro	Selector	Tasa	¿Reenvío?	¿Recopilación de datos?

- Definimos las clases que van a ocupar las políticas de QoS tomando en cuenta algunos aspectos:

  - Saber que niveles de servicios se están proporcionando a los clientes.

  - Que aplicaciones son las que generan mayor cantidad de tráfico en la red.

  - Que aplicaciones son la que proporcionan información con mayor prioridad.

  - Si se trabaja con un SLA se deben revisar los acuerdos que determinen el tipo de tráfico con el que se pretende trabajar y posteriormente que se los supervise.

- Enumeramos las clases ya definidas en la tabla y asignaremos un nivel de prioridad para cada clase.

La priorización de las clases se dará por niveles: máxima, media y baja prioridad. De tal manera el selector de prioridad de cada clase otorgara un nivel se servicio.

3. Definición de filtros para cada clase

La definición de filtros se basa en determinar de la mejor manera el modo de separar el tráfico de una clase específica del flujo del tráfico de la red.

Se pueden crear filtros para identificar flujos de paquetes como miembros de una clase específica.

Los filtros son conjuntos de reglas que involucran a los selectores. Cada filtro hace referencia a una clase, QoS utiliza los criterios de los selectores para comparar los paquetes de cada filtro y determinar que trato tendrá cada paquete.

Para crear filtros se seguirán los siguientes pasos:

- Crear un filtro para cada clase de la tabla de planificación de QoS mencionada anteriormente.

- Definir al menos un selector para cada filtro de una clase.

Clase	Prioridad	Filtro	Selector

4. Definición del control del flujo para cada clase del tráfico.

El control de flujo permite medir el flujo del tráfico de una clase y transferir los paquetes que pasan por la red. Al planificar el control de flujo se usarán módulos de medición para identificar aspectos como el ancho de banda.

Por lo tanto una vez definido los filtros y selectores, podemos continuar con el siguiente procedimiento:

- Determinaremos el ancho de manda necesario para la voz, recomendamos usar el 60% del ancho de banda como prioridad y el otro 40% de ancho de banda para los demás servicios y aplicaciones.

- Si el servicio de red está en los acuerdos de un SLA, debemos identificar qué tipo servicios y que tipo de clientes van a obtener estos beneficios.

- Si un SLA lo requiere se crearan nuevas clases con sus respectivas prioridades.

- Determinamos los filtros que serán asociados a cada clase del tráfico para el control de flujos. Algunas clases pueden ocupar un solo filtro.

- Elegimos un módulo de medición para cada clase del control del flujo

- Añadimos las tasas de medición para cada clase. Las tasas de medición se medirán en bits por segundo (bps).
    - Tasa asignada
    - Tasa máxima

La estructura de la tabla es la siguiente:

Clase	Prioridad	Filtro	Selector	Tasa

5. Definición del campo DSCP

A continuación vamos a definir los valores de prioridad del campo DSCP para poder aplicar las políticas de QoS. Por lo tanto debemos planificar un esquema donde determinará cómo se comporta el reenvío del flujo de datos que pasan por cada enrutador o nodo.

El comportamiento de reenvío dentro de la red se puede determinar por prioridad o por precedencia de descarte. La prioridad del flujo de tráfico se lo puede realizar diferenciado una clase de otra o precedencia de descarte que descarta los flujos por completo.

Aplicando el modelo Difserv existen dos formas de marcar el comportamiento de reenvío y son:

- Marcando el campo de DS del paquete IP con un DSCP

- Marcando la etiqueta de la VLAN de un datagrama con un valor de clase de servicio asignada.

Para priorizar el trafico IP, debemos asignar un punto DSCP a cada paquete. El DSCP de una clase determina el comportamiento de reenvío y se lo realizará a través de dos tipos de comportamientos PBH AF y PBH EF. Debemos tomar en cuenta una serie de pasos a seguir:

- Revisar las clases creadas y las prioridades asignadas a cada clase.

- Asignaremos el comportamiento por saltos EF a la clase con prioridad más alta.

PBH EF garantiza que los paquetes con DSCP EF se transfieran primero que los paquetes con comportamiento PBH AF. EF ofrece mayor prioridad para el tráfico.

Cuando los paquetes llegan a los enrutadores, éstos evalúan los puntos de código de los paquetes junto con los puntos de código DSCP de otro tráfico en cola. El enrutador es el encargado de reenviar los paquetes o descartarlos, dependiendo las prioridades asignadas o por el ancho de banda establecido. PBH EF garantiza el ancho de banda con respecto a los paquetes con comportamiento AF.

Cuando usamos dispositivos VLAN, los nodos de red pueden leer el campo de prioridad del datagrama del encabezado MAC.

- Asignamos los comportamientos del reenvío de clases que van a medirse.

- Asignamos los puntos de condigo DS al resto de clases según las prioridades de cada uno.

6. Plan de supervisión estadístico para los flujos de tráfico de red

Permite supervisar el flujo de tráfico que pasa por la red por motivos de administración de red o facturación para determinar si se necesitan recopilación de datos sobre el flujo, tomando en cuenta el siguiente proceso:

- Conocer si la empresa dispone de un SLA, si es afirmativo se deben recopilar los datos sobre el flujo para determinar que clases son las que se van a facturar y que tipo de servicio se va a proporcionar a los clientes de acuerdo a los puntos establecidos dentro del SLA.

- Debemos supervisar que no existan problemas en la red y verificar que tipo de clases necesitan supervisión.

5.1.3 Vulnerabilidad 3: Falta de un Sistema de Pruebas de Calidad de Voz

Otra vulnerabilidad encontrada dentro de la empresa CELEC EP TRANSELECTRIC es la falta de disponibilidad de un sistema de pruebas de calidad de voz, esto significa que junto con la QoS se evidencian los problemas existentes dentro del servicio telefónico.

Las pruebas de calidad de voz sirven para monitorear el sistema de telefonía en cuanto a su rendimiento y servicio que otorga a cada uno de los empleados de la empresa.

Los empleados concluyeron que finalmente están satisfechos con el servicio de telefonía, pero si es necesario que se realicen estas pruebas cada cierto tiempo.

Como última sugerencia de la misma forma que la anterior vulnerabilidad implemente un servicio donde sean capaces de controlar la red, en este caso mantener un servicio de telefonía aceptable sin problemas para todos los empleados y así disminuir los porcentajes evidenciados en las encuestas.

Para que se realice este tipo de servicios nos guiaremos un factor denominado “Calidad de Experiencia” (QoE) encargado de realizar estudios en base a la experiencia del usuario con el servicio con el que trabajan. A continuación vamos a estudiar detalladamente este tema.

5.1.3.1 Calidad de Experiencia (QoE)

La calidad de experiencia (QoE) se define como los usuarios finales perciben o tienen experiencia sobre el servicio que están teniendo y la calidad que éste les proporciona. Por lo tanto la calidad de experiencia refleja como los servicios de red satisfacen las necesidades de los usuarios finales. Hay que tomar muy en cuenta que la calidad de experiencia (QoE) y la calidad de servicio (QoS) son términos separados. La QoE analiza la experiencia que tiene el usuario con el servicio mientras que la QoS hacen referencia y al trato de los paquetes IP en la red. (Rouse, TechTarget, 2012)

Factores

- Los principales factores de éxito que influyen a la QoE son:

- Facilidad: Factor importante, los usuarios deben ser capaces de manipular el servicio

- Confiabilidad: El servicio proporcionado debe tener un nivel de disponibilidad y estabilidad

- Costo: El servicio a ofrecer debe tener un precio razonable para el usuario para mejorar el valor de la calidad de experiencia.

- Seguridad: Debe ofrecerse un alto nivel de seguridad en los datos del usuario para que no puedan sufrir ningún tipo de ataque en sus equipos e información.

- Calidad en los contenidos (Audio y Video): Hace referencia a la calidad de los contenidos multimedia que los usuarios perciben

- Lealtad al cliente: El usuario determina en base a su experiencia si el servicio es aceptable, para la empresa es muy importante saberlo.

(TechoPedia, s.f.)

Sistemas de medición de QoE

Cuando nos referimos a la comunicación por voz y video, la calidad puede ser buena o mala, por lo tanto, un mecanismo para poder medir la calidad de experiencia se denomina Mean Opinion Score (MOS)

5.1.3.1.1 MOS

Se considera una indicación numérica de la calidad percibida por la voz recibida después de haber sido transmitida y comprimida por los codecs. Esta medición se la realiza a través de redes subyacentes que actúan sobre el flujo de datos y de esta manera se puede verificar la calidad de las llamadas. Se considera una buena herramienta para sistemas de VoIP. (VoIPMechanic, 2015)

Factores que afectan las pruebas de VoIP con MOS

Antes de enumerar y explicar cuáles son los factores que afectan las pruebas de VoIP con MOS, es importante saber que MOS es una escala relativa y se basa en muchos factores que afectan la calidad de voz.

Las diferentes mediciones que se hacen en VoIP para probar si existe retardo o latencia, pérdida de paquetes, eco. Los siguientes elementos que afectan la calidad de llamada son:

- Latencia
- Ancho de banda
- Eco
- El códec que se está utilizando
- Hardware utilizado
- Jitter
- Paquetes perdidos

Retardo de propagación: Es el tiempo que se necesita cuando una señal digital pasa de extremo a extremo a través de la red. El paso de los paquetes es a través de routers, switches, cortafuegos, por lo tanto, mientras mayor sea la distancia, mayor será el retardo de propagación. (VoIPMechanic, 2015)

Retraso de paquetización: Es el tiempo que se necesita para digitalizar la señal para el códec utilizado. El códec G.729 tiene más retraso de paquetización que el códec G.711

Codec: Es el encargado de convertir la señal a formato digital para que luego sea transmitida y reproducida. Codec también comprime el paquete para obtener una máxima eficiencia de la red.. (ThwackCommunity, 2015)

MOS haca más énfasis a los codecs, ya que los codecs son los encargados de comprimir el audio y video para ahorrar en la utilización del ancho de banda.

Valores de puntuación del MOS

Gracias a esta herramienta MOS dentro de las empresas ya la calidad de voz se mantiene sin ningún problema. Por lo tanto, es necesario llevar una métrica para medir los cambios de la calidad de voz, identificar los problemas y tratar de solucionarlos. Un rango que se le da a la VoIP es de 3.5 a 4.2 según MOS.

La siguiente tabla muestra una serie características y valores para guiarnos en las pruebas de VoIP MOS y una buena comparación con la calidad de voz.

Calidad de Llamadas	MOS
4.3-5.0	Muy Satisfecho
4.0-4.3	Satisfecho
3.6-4.0	Algunos usuarios satisfechos
3.1-3.6	Muchos usuarios insatisfechos
2.6-3.1	Casi todos los usuarios insatisfechos
1.0-2.6	No recomendado

Monitoreo de la QoE

La calidad de experiencia (QoE) está basada en Estándares y Normas para mediciones de calidad de los servicios como es el caso de MOS.

Por lo tanto, para poder mantener un monitoreo de la red debemos controlar la transmisión de datos y establecer correctamente la QoS. La arquitectura de un sistema de monitoreo de redes IP se basa en el despliegue de sondas encargadas de recolectar la información.

Las sondas se basan en la topología de la red basada en parámetros como el ancho de banda, la distribución de datos logrando determinar en tiempo real la supervisión de red. El control y operaciones de red actúan sobre elementos de la red que son los routers. (Bonini, 2012)

Existen varias aplicaciones que se pueden obtener para poder realizar éste tipo de análisis y otras aplicaciones que se pueden obtener por medio de empresas proveedoras y con SLA.

Como ejemplo se usó una imagen de la aplicación NGenius Video Monitorin Solution para verificar como funciona.

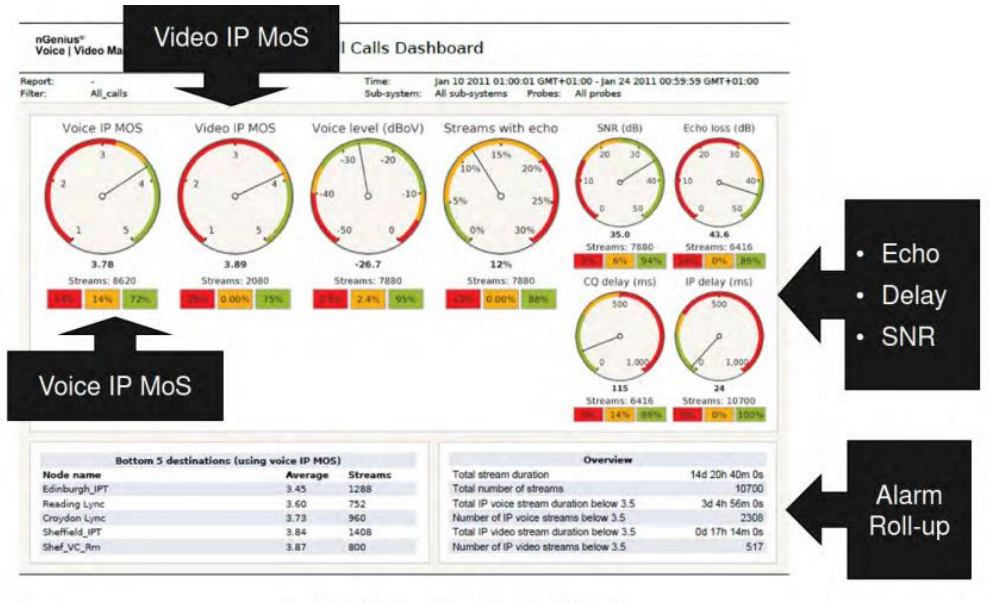


Figura 5.1.3.1 Ejemplo Aplicación NGenius

(Bonini, 2012)

Figura 5.1.3.2 Ejemplo Aplicación NGenius

(Bonini, 2012)

Consideraciones a tomar en cuenta

Para mantener establece una comunicación y la buena implementación de la telefonía IP se considera usar buenos equipos que soporten este tipo de características, usar el correcto uso de los codecs como el G729 o G711 y la buena administración de las redes.

El costo de afinamiento y mejoramiento de la experiencia de usuario se detallada y considera en 2 rubros:

- ✓ En el precio de la instalación y pruebas previas a la entrega del proyecto.
- ✓ Es parte del servicio de soporte y mantenimiento que recibe la plataforma año a año.

Finalmente, se sugiere que se realicen pruebas de mantenimiento para gestionar la red, en nuestro caso pruebas de calidad de voz y adicionalmente mantenimiento de los equipos ya existentes. Se recomienda realizar este proceso cada 4 o 6 meses para mantener un correcto funcionamiento y satisfacción tanto de los usuarios como de la empresa en general.

6 Capítulo VI: Conclusiones y Recomendaciones

6.1 Conclusiones

1. Disponer de una central espejo se considera una solución rápida y viable en caso de que la actual central telefónica llegue a dañarse, por otro lado, el análisis económico realizado indica que los costos del equipo junto con sus licencias y repuestos son valores altos. Adicionalmente, tomando en cuenta que este tipo de centrales tienen una sola vida útil, es conveniente tener un contrato de servicios de mantenimiento, soporte y configuraciones la cuál sería más conveniente para cuidar los equipos pero la decisión quedará en manos de la empresa.

2. La empresa CELEC EP – TRANSELECTRIC dispone actualmente de un contrato con requerimientos que cubren los servicios de mantenimiento y soporte técnico, pero no disponen de un contrato que indique ciertas necesidades como es el caso de la central telefonía con sus respectivas licencias y repuestos.

3. El servicio de telefonía IP dentro de la empresa es considerado un aspecto indispensable ya que su trabajo se basa en la comunicación con todas las unidades de negocio en del país, incluye la comunicación interna e internacional lo que hace que la calidad de servicio llegue a ser un factor decisivo para la comunicación.

4. Los resultados de las encuestas aplicadas a los empleados junto con los conocimientos adquiridos acerca de las seguridades de voz sobre IP se puede concluir que la empresa mantiene un estable sistema de seguridad al no sufrir algún tipo de ataque. Por otro lado, se comprueba que existen ciertos inconvenientes en la comunicación de la telefonía IP y la falta de un sistema de calidad de servicio.

5. Se puede concluir que la implementación de un sistema de calidad de servicio aportará varias ventajas a favor de la empresa, la comunicación entre los empleados mejorará notablemente, se reducirán los porcentajes de inconvenientes obtenidos en las encuestas, cabe recalcar que no solamente los inconvenientes son debidos directamente a la comunicación sino que puede existir fallas en los equipos que pueden solucionarse rápidamente.

6.2 Recomendaciones

1. Es recomendable disponer de una o varias personas responsables, preparadas y capaces de solucionar problemas tanto hardware como software lo más rápido posible.

2. Se recomienda implementar un sistema de calidad de servicio para optimizar la comunicación dentro de la empresa y mejorar el rendimiento de los empleados.

3. Es recomendable conservar un monitoreo del tráfico de la red cada cierto tiempo para evitar cualquier tipo de percance y tener todo correctamente.

4. Se recomienda realizar auditorías de mejora continua en base a procesos de calidad sobre la red actual con la que disponen.

7 Glosario

C

Circuitos conmutados
Son aquellos que envían información a través de un canal no compartido, formado por un camino a todo lo largo de la llamada telefónica 17

E

Enrutar
Redirigir una conexión a un equipo que dispone de un servicio específico o un software que necesita realizar conexiones 22

Ethernet
Estándar de conexión a la red Internet 28

G

GPL
Licencia orientada a proteger la libre distribución, modificación y uso del software . 12

H

HTTP
Protocolo de transferencia que se encarga de enviar información entre el servidor y los clientes 25

I

IPSec
Usa los servicios de seguridad de tráfico para proteger las comunicaciones usando el protoclo IP 23

J

Jitter buffer
Es un área de datos compartida donde los paquetes de voz se pueden recoger, almacenar y ser enviados al procesador de voz en intervalos de tiempos iguales.. 9

P

PBX
Red telefónica privada que se utiliza dentro las empresas, los usuarios de la central telefónica PBX comparten números definidos de líneas telefónicas 12

S

Señalización
Permite el intercambio de información entre los usuarios y la red, con el fin de que la llamada pueda ser establecida y posteriormente terminada 41

SMTP
Protocolo estándar de Internet para el intercambio de correo electrónico, se necesita de tres datos origen, destino y medio (servidor) 25

SSL
Protocolo de seguridad que se utiliza para realizar conexiones seguras con el cliente y el servidor 23

8 Bibliografía

1. *3CX*. (s.f.).

   Obtenido de http://www.3cx.es/voip-sip/sip-call-session/

2. Alvarez, V. A. (2007).

   Análisis y definición de un mecanismo basado en servicios diferenciados para ofrecer calidad de servicio en redes IP. Escuela Politécnica del Ejercito. Recuperado el 22 de 08 de 2015

3. (2012).

   Arquitectura de Calidad de Servicios DiffServ e IntServ. Presentación Power Point, Departamento de Sistemas Telemáticos y Computación (GSyC). Recuperado el 16 de 09 de 2015, de http://es.slideshare.net/c09271/2-2diff-servintserv

4. *ASIR.* (22 de 05 de 2015).

   Obtenido de http://www.asirsl.com/images/DossierSLA.pdf

5. *Asterisk*. (s.f.).

   Obtenido de http://www.asterisk.org/get-started/applications/pbx

6. *BidDigital.* (2015).
   Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/4166/1/CD-0729.pdf

7. *Black Kernel.* (12 de 11 de 2012).

   Obtenido de http://4lfa-om3ga.blogspot.com/2012/11/como-detectar-y-evitar-un-arp-spoofing.html

8. Bonini, J. (30 de 05 de 2012).

   Recuperado el 17 de 09 de 2015, de http://www.ieee.org.ar/downloads/bonini-qox-en-redes-de-video-sobre-ip.pdf

9. *BYTECODERS*. (07 de 05 de 2010).

   Obtenido de http://bytecoders.net/content/ataques-voip.html

10. *Calidade servicios (QoS)*. (21 de 08 de 2014).

Obtenido de http://www.uv.es/~montanan/ampliacion/ampli_6.pdf

11. *CISCO*. (s.f.). Obtenido de http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html

12. *CISCO*. (04 de 12 de 2006). Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CDYQFjAD&url=http%3A%2F%2Fwww.cisco.com%2Fweb%2Fabout%2Fac123%2Fac147%2Farchived_issues%2Fipj_10-4%2F104_ip-spoofing.html&ei=fH2RVdjWNYvn-QHSmJfYCw&usg=AFQjCNG6FPCZsLgD

13. CUEVA, M. (10 de 07 de 2012). Obtenido de Monografías: http://www.monografias.com/trabajos87/voz-ip/voz-ip.shtml

14. *DanySoft.* (2013). Obtenido de http://www.danysoft.com/free/reservarecursos.pdf

15. *Data Network Resource*. (s.f.). Obtenido de http://www.rhyshaden.com/qos.htmD

16. Delfino, A., & Rivero, S. (s.f.). *Monografía de Evaluación de Performance en Redes de Telecomunicaciones.* Monografía. Obtenido de http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

17. *Elastictech*. (s.f.). Obtenido de http://elastixtech.com/qos-calidad-de-servicio-para-voip/

18. *ElastixTech.* (s.f.). Obtenido de Protocolo SIP: http://elastixtech.com/qos-calidad-de-servicio-para-voip/

19. *Endebian*. (30 de 01 de 2013).

Obtenido de https://endebian.wordpress.com/2013/01/30/arp-poisoning-envenenamiento-arp/

20. *Estudio de priorización de tráfico para VoIP*. (2013).

Obtenido de http://www.vilarrasa.com.ar/qos_para_voip.htm

21. *Expresion Binaria*. (18 de 10 de 2013).

Obtenido de http://www.expresionbinaria.com/ataque-de-tipo-arp-spoofing/

22. *Gemini Security Solutions*. (08 de 12 de 2008).

Obtenido de http://securitymusings.com/article/tag/arp-spoofing

23. *Guimi.net.* (2009).

Obtenido de http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf

24. GUTIERRREZ, J. (Dirección). (2011).

Instalacion de central telefonica [Película].

25. HAUGHN, M. (08 de 2014).

Whatls.com. Obtenido de http://whatis.techtarget.com/definition/multipoint-control-unit-MCU

26. HERRANZ, A. (13 de 07 de 2007).

PCWorld. Obtenido de http://www.pcworld.es/seguridad/el-phishing-se-traslada-a-la-voip-y-a-la-telefonia-movil

27. HUARCAYA, J. (Dirección). (2014).

Tecnología VoIP [Película].

28. *itprocessMaps.* (04 de 08 de 2013).

Obtenido de http://wiki.es.it-processmaps.com/index.php/Lista_de_control_-_SLA_OLA_UC

29. *Juniper Networks*. (20 de 05 de 2015).

Obtenido de https://translate.google.com.ec/translate?hl=es&sl=en&u=http://www.juniper.net/techpubs/hardware/mx960/mx960-dpc/mx960-dpc.pdf&prev=search

30. *Juniper Networks*. (19 de 05 de 2015).

Obtenido de http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx480/

31. KAREN, A., & FABIAN, A. (Dirección). (2013).

Modelo TCP/IP [Película].

32. Luz, S. d. (04 de 08 de 2012).

Redes@Zone. Obtenido de http://www.redeszone.net/2011/08/04/la-capa-de-red-volumen-iv-ipv4/

33. *Manual Técino Siemens HIPATH.* (2007).

Obtenido de http://mfcom.es/HIPATH%203000-5000%20V7%20TECNICO.pdf

34. Martinez, J. (s.f.).

Calidad de Servicios (QoS). Presentacion Power Point, Universidad Javeriana de Cali, Cali. Recuperado el 16 de 09 de 2015, de http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_-_calidad_de_servicio_qos_.pdf

35. *Module 7: What is IP Spoofing?* (2015).

[Película]. Obtenido de https://www.youtube.com/watch?v=zopRwR0yhlg

36. Montañana, R. (2013).

Calidad de Servicio (QoS). Obtenido de http://www.uv.es/~montanan/ampliacion/ampli_6.pdf

37. *MuyPymes*. (09 de 2014).

Obtenido de http://www.muypymes.com/2014/09/09/aplicaciones-voip

38. NAVEEN. (s.f.).

SlideShare. Obtenido de http://www.slideshare.net/akmalh8/ip-spoofing-34258568

39. *Networld.* (01 de 04 de 2002).

Obtenido de http://www.networkworld.es/archive/sla-que-son-para-que-sirven

40. *Norton by Symantec*. (2015).

Obtenido de http://mx.norton.com/voip-security-a-primer/article

41. NOVILLO, F. (12 de 06 de 2008).

Wordpress. Obtenido de https://rovitor.wordpress.com/2008/06/11/protocolos-para-contenido-enriquecido/

42. Peñafiel, H. E. (2005).

ESTUDIO TECNICO DEL CONTROL DE CALIDAD DE LOS. PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA ELECTRÓNICA, Escuela Plotécnica del Ejercito, Quito.

43. PEREZ, A. (s.f.).

*Scribd.*Obtenido de https://es.scribd.com/doc/52385782/75/Hibridos-y-supresores-de-eco

44. PUEBLA, M. (04 de 2010).

Scrib. Obtenido de http://es.scribd.com/doc/34037049/Protocolo-SIP#scribd

45. *RAINI COMPUTER*. (s.f.).

Obtenido de http://www.raini.es/informacion_telefonia_ip.html

46. *Redes Convergentes: Internet de las cosas*. (22 de 07 de 2014).

Obtenido de https://rcicesi.wordpress.com/2014/10/22/una-mirada-a-los-servicios-de-las-redes-convergentes-voip/

47. *Redes de Comunicaciones.* (2009).

Obtenido de http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf

48. Romero, S. (6 de Mayo de 2004).

Obtenido de La Flecha: http://www.laflecha.net/articulos/seguridad/voip

49. Rouse, M. (04 de 2012).

TechTarget. Obtenido de http://searchcrm.techtarget.com/definition/Quality-of-Experience

50. Rouse, M. (23 de 04 de 2015).

Search IT Channel. Obtenido de http://searchitchannel.techtarget.com/definition/service-level-agreement

51. RUIZ, A. (13 de 10 de 2007).

VSAntivirus. Obtenido de http://www.vsantivirus.com/phishing-skype-131007.htm

52. Salinas, A. (s.f.).

QoS: Garantía de Eficiencia en redes de datos. Presentacion Power Point, Univerdidad Católica Popular de Risaralda, Ingeniería en Sistemas y Telecomunicaciones . Obtenido de http://es.slideshare.net/exactlimon/presentaciones-andres-salinas

53. SALVADOR, O. (Dirección). (2013).

Como Funciona una Central Telefonica ¿Quieres aprender más de telefonia? [Película].

54. *Security ATWORK*. (14 de 03 de 2008).

Obtenido de http://www.securityartwork.es/2008/03/14/eavesdropping-en-voip/

55. *Security By Default*. (13 de 09 de 2012).

Obtenido de http://www.securitybydefault.com/2012/09/riesgos-reales-en-voip.html

56. *Soluciones IT*. (2015).

Obtenido de http://solucionesit.wikispaces.com/-/Srvs015/VoIP/Asterisk

57. *Symantec*. (11 de 03 de 2003).

Obtenido de http://www.symantec.com/connect/articles/ip-spoofing-introduction

58. *TechoPedia*. (s.f.)

Recuperado el 16 de 09 de 2015, de https://www.techopedia.com/definition/25802/quality-of-experience-qoe

59. *Telecomunicaciones para Gerentes*. (31 de 03 de 2014).

Obtenido de http://www.telecomunicacionesparagerentes.com/cual-es-el-mejor-codec-para-voip/

60. *Telefonía Voz IP*. (s.f.).

Obtenido de http://www.telefoniavozip.com/voip/ventajas-de-la-telefonia-ip.htm

61. Ternero, D. M. (2010).

Calidad de Servicios en Redes (QoS). Presentación Power Point, Universidad de Sevilla, Departamento de tecnología Electrónica. Obtenido de http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf

62. *ThwackCommunity*. (2015).

Obtenido de https://thwack.solarwinds.com/community/solarwinds-community/geek-speak_tht/blog/2014/04/15/how-does-mean-opinion-score-measure-voip-performance

63. Unify. (2013).

HiPath 4000 Assitant/Manager Backup/Restore.

64. *University Credit Union.* (s.f.).

Obtenido de http://www.ucumiami.org/index.php?option=com_content&view=article&id=241&Itemid=175&lang=es

65. VILLAREAL, M. (2006).

Monografias. Obtenido de http://www.monografias.com/trabajos33/estandar-voip/estandar-voip2.shtml

66. *VoipForo*. (s.f.).

Obtenido de 3CX: http://www.voipforo.com/SIP/SIPcomponentes.php

67. *VoIPForo.* (s.f.).

Recuperado el 23 de 09 de 2015, de http://www.voipforo.com/QoS/QoS_PacketLoss.php

68. *VoIPMechanic*. (17 de 09 de 2015).

Obtenido de http://www.voipmechanic.com/mos-mean-opinion-score.htm

69. *Wikipedia*. (27 de 09 de 2012).

Obtenido de http://wiki.sj.ifsc.edu.br/wiki/index.php/RMU-2012-1

70. *Wikipedia*. (5 de 07 de 2015)

Obtenido de https://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet

71. *ZonaVirus*. (13 de 12 de 2001).

Obtenido de http://www.zonavirus.com/articulos/que-es-el-spoofing.asp